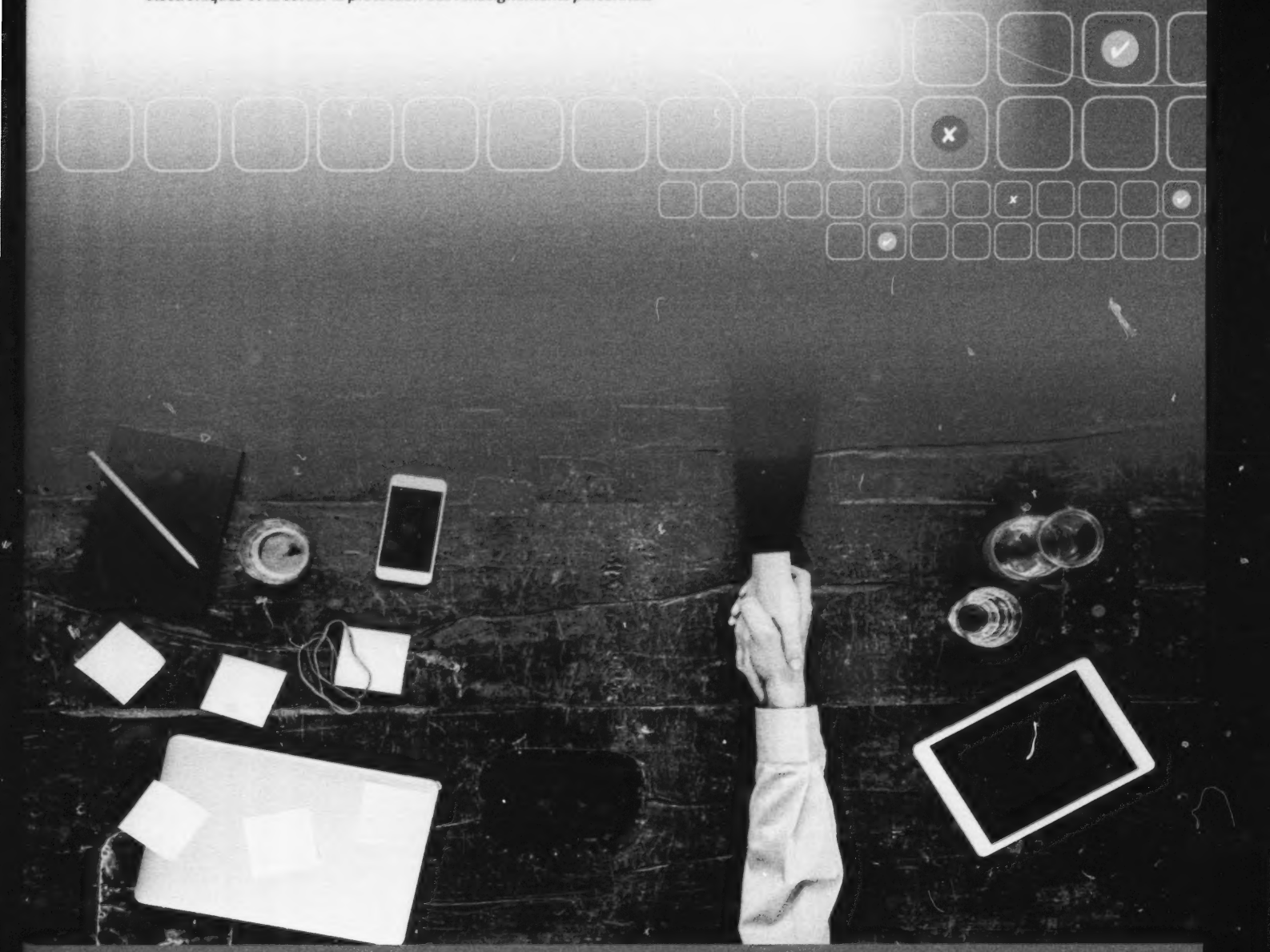
Commissariat
à la protection de
la vie privée du Canada

Rapport annuel au Parlement 2017–2018

concernant la *Loi sur la protection des renseignements personnels et les documents électroniques* et la *Loi sur la protection des renseignements personnels*



FAIRE CONFIANCE MAIS **VÉRIFIER**

La confiance dans l'économie numérique passe par une réelle surveillance indépendante

Rapport annuel au Parlement 2017-2018 concernant la *Loi sur la protection des renseignements personnels et les documents électroniques* et la *Loi sur la protection des renseignements personnels*

Faire confiance mais vérifier
La confiance dans l'économie numérique passe par une réelle surveillance indépendante

Commissariat à la protection de la vie privée du Canada
30, rue Victoria
Gatineau (Québec) K1A 1H3

© Sa Majesté la Reine du chef du Canada pour le Commissariat à la protection de la vie privée du Canada, 2018
Numéro de catalogue : IP51-1F-PDF
Numéro ISSN : 1913-3375

Suivez-nous sur Twitter : @PriveePrivacy
Facebook : https://www.facebook.com/ViePriveeCanada/

Commissaire à la protection de la vie privée du Canada

30, rue Victoria
Gatineau (Québec)
K1A 1H3
Tél. : (819) 994-5444
1 800 282-1376
www.priv.gc.ca

Privacy Commissioner of Canada

30 Victoria Street
Gatineau, Quebec
[illegible]
[illegible]994-5444
1-800-[illegible]1376
www.priv.gc.ca

L'honorable George J. Furey, sénateur
Président
Sénat du Canada
Ottawa (Ontario) K1A 0A4

Septembre 2018

Monsieur,

J'ai l'honneur de remettre au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada pour la période du 1er avril 2017 au 31 mars 2018. Ce dépôt se fait en vertu des articles 38 de la *Loi sur la protection des renseignements personnels et les documents électroniques* et 25 de la *Loi sur la protection des renseignements personnels*.

Je vous prie d'agréer, Monsieur, l'assurance de ma considération distinguée.

Le commissaire,

Original signé par

Daniel Therrien

Commissaire à la protection de la vie privée du Canada

30, rue Victoria
Gatineau (Québec)
K1A 1H3
Tél. : (819) 994-5444
1 800 282-1376
www.priv.gc.ca

Privacy Commissioner of Canada

30 Victoria Street
Gatineau, Quebec
K1A 1H3
Tel.: (819) 994-5444
1 800 282-1376
www.priv.gc.ca

L'honorable Geoff Regan, député
Président
Chambre des communes
Ottawa (Ontario) K1A 0A6

Septembre 2018

Monsieur,

J'ai l'honneur de remettre au Parlement le rapport annuel du Commissariat à la protection de la vie privée du Canada pour la période du 1er avril 2017 au 31 mars 2018. Ce dépôt se fait en vertu des articles 38 de la *Loi sur la protection des renseignements personnels et les documents électroniques* et 25 de la *Loi sur la protection des renseignements personnels*.

Je vous prie d'agréer, Monsieur, l'assurance de ma considération distinguée.

Le commissaire,

Original signé par

Daniel Therrien

Table des matières

Message du commissaire 1
- La crise de Facebook et Cambridge Analytica 1
- Des progrès lents, voire inexistants, réalisés par le gouvernement 3
- Lignes directrices sur le consentement valable et sur les pratiques inacceptables 4
- Réputation 5
- Une vision proactive de la protection de la vie privée 6
- Mot de la fin 9

La protection de la vie privée en chiffres 11

Loi sur la protection des renseignements personnels et les documents électroniques – Rétrospective de l'exercice 13
- Consentement et contrôle 13
- Enquêtes en vertu de la LPRPDE en général 26
- Activités parlementaires liées à la LPRPDE 34
- Programme des contributions 38

Loi sur la protection des renseignements personnels – Rétrospective de l'exercice 41
- Sécurité nationale 41
- La vie privée à la frontière 42
- Réforme de la *Loi sur la protection des renseignements personnels* et activités parlementaires 45
- Enquêtes en vertu de la *Loi sur la protection des renseignements personnels* 47
- Avis au gouvernement 60

Dossiers relatifs à la protection de la vie privée devant les tribunaux 71
- Dossiers auxquels le Commissariat a participé au cours de l'exercice écoulé 71
- Dossiers que nous avons suivis avec intérêt 73

Coopération avec des organisations canadiennes et internationales 75
- Conférence internationale des commissaires à la protection des données et de la vie privée 75
- Autorités de protection de la vie privée de la zone Asie-Pacifique 76
- Global Privacy Enforcement Network (GPEN) 76
- Loi canadienne anti-pourriel (LCAP) 77
- Coopération fédérale-provinciale-territoriale 77
- Mobilisation proactive à l'égard du SS7 78

Annexe 1 – Définitions 79

Annexe 2 – Tableaux statistiques 82
- Statistiques relatives à la LPRPDE 82
- Tableaux statistiques liés à la *Loi sur la protection des renseignements personnels* 89

Annexe 3 – Processus d'enquête 102
- Processus d'enquête en vertu de la LPRPDE 102
- Processus d'enquête en vertu de la *Loi sur la protection des renseignements personnels* 104

Annexe 4 – Rapport du commissaire spécial à la protection de la vie privée pour 2017-2018 106

Message du commissaire

La crise de Facebook et Cambridge Analytica

Pour opérer un changement, il faut parfois une crise. Or, les crises n'ont pas manqué au cours de l'exercice écoulé dans le domaine de la protection de la vie privée.

Les atteintes à la sécurité des données, malheureusement trop courantes, ont cette fois touché des millions de clients d'entreprises comme Equifax, Uber et Nissan Canada Finance. Il y a bien évidemment aussi l'affaire Facebook et Cambridge Analytica, sur laquelle nous faisons enquête à l'heure actuelle. Ce cas est largement perçu comme un sérieux rappel à l'ordre qui a mis en évidence la crise de plus en plus grave frappant le droit à la vie privée.

L'affaire Facebook a obligé les Canadiens à constater que leurs renseignements personnels peuvent être analysés à des fins bien plus insidieuses que le marketing. Dans ce cas, des renseignements d'utilisateurs auraient été utilisés pour influencer des opinions politiques. À quoi faut-il s'attendre maintenant? De quelles autres façons nous manipule-t-on?

Ces enjeux montrent aussi les lacunes des lois canadiennes sur la protection des renseignements personnels sur lesquelles moi-même et mes prédécesseurs avons tenté d'attirer l'attention depuis des années. Uniquement au cours du dernier exercice, nous avons eu de nombreuses possibilités de mettre ces lacunes en évidence et de proposer des pistes de solution.

Nous avons comparu devant les parlementaires et leur avons présenté des mémoires pour faire valoir la nécessité de moderniser la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). Nous avons aussi proposé des modifications à la législation sur la sécurité nationale, soit le projet de loi C-59, en reprenant entre autres plusieurs recommandations que nous avions formulées concernant la réforme de la *Loi sur la protection des renseignements personnels* en 2016.

Nous avons également attiré l'attention sur le manque de normes et de surveillance en ce qui concerne les pratiques de traitement des renseignements personnels adoptées par les partis politiques. Le gouvernement a déposé le projet de loi C-76, qui vise à combler cette lacune importante.

Toutefois, ce projet de loi n'ajoute rien au chapitre de la protection de la vie privée. En fait, au lieu d'imposer des normes reconnues à l'échelle internationale, il laisse aux partis le soin de définir les règles qu'ils souhaitent appliquer. De plus, il n'impose aucun mécanisme de surveillance indépendant. Sur ce plan et à bien d'autres égards, les lois canadiennes sur la protection des renseignements personnels ne sont malheureusement pas à la hauteur des protections en vigueur dans d'autres pays.

Les Canadiens veulent profiter des nombreux bienfaits de l'économie numérique, mais ils s'attendent à juste titre à pouvoir le faire tout en sachant que leurs droits seront protégés par des lois efficaces et que leurs renseignements personnels ne seront pas utilisés contre eux. Ils veulent avoir confiance que les règles, les lois et le gouvernement les protégeront contre d'éventuels préjudices.

On peut faire confiance dans une certaine mesure, mais il faut aussi vérifier. Pour renforcer la confiance dans l'économie numérique, nous devons veiller à ce que les Canadiens puissent compter sur un tiers indépendant pouvant vérifier la conformité aux lois sur la protection des renseignements personnels.

Le temps de l'autoréglementation est terminé. Bien sûr, au Canada, nous avons des lois relatives à la protection de la vie privée. Mais celles-ci sont très permissives et accordent aux entreprises une grande latitude en ce qui concerne l'utilisation des renseignements personnels dans leur propre intérêt. En vertu de la LPRPDE, les organisations doivent respecter le principe de responsabilité, mais les Canadiens ne peuvent se fier exclusivement aux entreprises pour gérer leurs renseignements de façon responsable. La transparence et la responsabilité sont nécessaires, mais elles ne sont pas suffisantes.

Pour être clair, il ne suffit pas de demander aux entreprises d'être à la hauteur de leurs responsabilités. Les Canadiens ont besoin de lois plus strictes en matière de protection des renseignements personnels qui les protégeront lorsque les organisations échoueront à le faire. Le respect de ces lois doit être assuré par un organisme de réglementation indépendant de l'industrie et du gouvernement et investi de pouvoirs suffisants pour assurer la conformité.

Compte tenu de l'opacité des modèles d'affaires et de la complexité des flux de données à l'ère de l'analyse des données, de l'intelligence artificielle et de l'Internet des objets, les consommateurs ne sont pas toujours en mesure d'identifier les pratiques pouvant leur porter préjudice et de porter plainte. L'organisme de réglementation, c'est-à-dire le Commissariat à l'échelle fédérale, devrait être autorisé à examiner les pratiques des organisations pour s'assurer de leur légalité, sans qu'une infraction à la loi soit forcément soupçonnée.

Autrement dit, on peut faire confiance dans une certaine mesure, mais il faut aussi vérifier. Pour renforcer la confiance dans l'économie numérique, nous devons veiller à ce que les Canadiens puissent compter sur un tiers indépendant pouvant vérifier la conformité aux lois sur la protection des renseignements personnels.

Nous avons également demandé au Parlement de se pencher sur la question du déréférencement et de l'effacement à la source en vue d'assurer le juste équilibre entre le droit à la réputation et à la vie privée, la liberté d'expression et l'intérêt public.

En ce qui concerne le secteur public, nous avons proposé des modifications au projet de loi C-59 en vue d'établir un meilleur équilibre entre la sécurité nationale et le respect de nos droits fondamentaux, notamment le droit à la vie privée.

Des progrès lents, voire inexistants, réalisés par le gouvernement

Plusieurs parlementaires ont appuyé notre appel en faveur d'une réforme des lois. Entre autres, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI) de la Chambre des communes, qui est chargé d'examiner les lois canadiennes sur la protection des renseignements personnels, a accepté en février 2018 bon nombre de nos recommandations visant à modifier la LPRPDE. Il a même réclamé des mesures supplémentaires s'inspirant du *Règlement général sur la protection des données* de l'Union européenne, qui est entré en vigueur en mai.

Dans un rapport publié ultérieurement en juin, après avoir entendu les témoignages sur l'affaire Facebook et Cambridge Analytica, le Comité ETHI a jugé qu'il était urgent d'apporter certains changements (en particulier pour conférer au Commissariat de nouveaux pouvoirs d'application de la loi, notamment le pouvoir de mener des inspections ou des vérifications). Le Comité estime aussi que les partis politiques devraient être assujettis aux lois sur la protection des renseignements personnels.

Malheureusement, les progrès réalisés par le gouvernement sont lents, voire inexistants. Le seul progrès véritable a consisté dans l'acceptation par le gouvernement de la plupart des modifications que nous avons proposées au projet de loi C-59, soit le projet de loi antiterroriste. En ce qui concerne la *Loi sur la protection des renseignements personnels*, adoptée il y a 35 ans pour réglementer la protection de la vie privée dans le secteur public, la ministre de la Justice a annoncé en 2016 qu'elle avait demandé à ses fonctionnaires de lancer d'intenses travaux de modernisation de la loi. Selon elle, ce projet s'imposait depuis longtemps. Aucune proposition concrète à cet égard n'a toutefois été présentée au public jusqu'à présent.

À la fin de juin 2018, le gouvernement a répondu aux recommandations du Comité ETHI visant à modifier la LPRPDE. Le ministre de l'Innovation, des Sciences et du Développement économique (ISDE) a convenu qu'il faut apporter des changements à notre régime de protection de la vie privée. Il a cependant soutenu que d'autres études s'imposent pour examiner la viabilité de toutes les options, par exemple les modèles d'application de la loi, afin de présenter des propositions aux Canadiens. Le ministre a lancé des consultations nationales sur le numérique et les données, qui pourraient aboutir à d'éventuelles modifications législatives dans plusieurs années.

Les Canadiens n'ont pas le luxe d'attendre plusieurs années afin qu'on remédie aux lacunes connues dans les lois sur la protection des renseignements personnels. La technologie évolue à un rythme effréné et plusieurs nouvelles technologies perturbent non seulement les modèles d'affaires, mais aussi les normes de la société et du droit. Il importe de mettre à jour ces normes rapidement pour que la confiance des consommateurs atteigne les niveaux désirés et que leurs droits soient protégés. Comme l'a fait remarquer le Comité ETHI dans son rapport en juin dernier, « on ne peut trop insister sur l'urgence de la situation ».

Évidemment, nous ne prétendons pas que la société soit parvenue au point où tous les risques d'atteinte à la vie privée sont connus et les mesures de protection sont parfaitement identifiées. Les consultations annoncées par le gouvernement ont donc une certaine justification. Toutefois, plusieurs améliorations souhaitables ont été identifiées depuis longtemps, dont le besoin de doter le Commissariat à la protection de la vie privée des pouvoirs nécessaires.

Nous savons que les Canadiens veulent ce changement et que les organisations préféreraient en général ne pas faire face à des inspections, des ordonnances et des sanctions pécuniaires. Nul n'est besoin de consulter sur cette question. Le moment est venu de passer à l'action.

Nous avons donc trouvé décevante la réponse du gouvernement, mais nous n'avons pas attendu le gouvernement pour agir. Nous avons entrepris plusieurs initiatives dans des domaines où nous exerçons un certain contrôle. Il s'agit cependant de lignes directrices et non pas de lois, si bien que la protection ainsi offerte aux Canadiens est limitée.

Lignes directrices sur le consentement valable et sur les pratiques inacceptables

L'an dernier, nous avons indiqué dans notre rapport annuel que le consentement devrait continuer à jouer un rôle important dans la protection de la vie privée au 21e siècle, car il demeure au cœur de l'autonomie personnelle. Le consentement occupe une place importante dans la protection de la vie privée dans les situations où la personne concernée dispose d'information suffisante pour donner un consentement valable.

Dans certains cas, toutefois, il est pratiquement impossible d'obtenir le consentement – par exemple dans certaines situations comportant l'utilisation de l'intelligence artificielle où les données peuvent servir à des fins multiples qui ne sont pas toujours connues au moment de leur collecte. D'autres méthodes de protection des renseignements personnels peuvent alors être requises. Nous avons également déterminé qu'il faut dans toutes les situations des mécanismes de soutien supplémentaires, notamment, des organismes de réglementation indépendants qui renseignent les citoyens, orientent l'industrie, lui demandent des comptes et sanctionnent les comportements inacceptables.

Pour mieux guider l'industrie et aider les personnes à exercer leur droit à la vie privée, nous avons publié en mai 2018 deux importants documents, soit les Lignes directrices pour l'obtention d'un consentement valable et le Document d'orientation sur les pratiques inacceptables du traitement des données. Ils ont été produits à l'issue d'une vaste consultation qui a notamment permis aux intervenants d'exprimer leur opinion sur les versions provisoires de ces documents publiées à l'automne.

Les lignes directrices sur le consentement présentent des conseils aux organisations pour s'assurer qu'elles obtiennent un consentement valable. Elles expliquent sept principes directeurs, notamment la nécessité de mettre l'accent sur quatre éléments clés dans les avis de confidentialité :

- les renseignements personnels qui seront recueillis;
- les tiers auxquels les renseignements personnels seront communiqués;
- les fins auxquelles les renseignements personnels seront recueillis, utilisés ou communiqués;
- le risque résiduel important de préjudice grave.

Le document d'orientation sur les pratiques inacceptables présente aux entreprises les pratiques inappropriées même avec le consentement des intéressés et renseigne les personnes sur les interdictions généralement imposées aux organisations. Mentionnons :

- un profilage donnant lieu à un traitement discriminatoire en vertu des lois sur les droits de la personne;
- la collecte, l'utilisation ou la communication de renseignements personnels à des fins qui causent ou sont susceptibles de causer un préjudice probable et grave à la personne;
- la publication de renseignements personnels dans le but de réclamer un paiement pour les retirer.

Nous avons élaboré nos *Lignes directrices pour l'obtention d'un consentement valable* en collaboration avec les commissariats à l'accès à l'information et à la protection de la vie privée de l'Alberta et de la Colombie-Britannique. Elles n'entreront en vigueur que le 1er janvier 2019, car nous souhaitons laisser aux organisations le temps voulu pour modifier leurs systèmes et pratiques. Le *Document d'orientation sur les pratiques inacceptables du traitement des données* est entré en vigueur en juillet 2018.

En général, les documents énoncent une combinaison d'exigences prévues par la loi et de pratiques exemplaires qui précisent nos attentes concernant ce qu'implique la conformité. Une fois les lignes directrices en vigueur, le Commissariat exercera ses activités dans cette optique.

Je sais que certains intervenants avaient des préoccupations au sujet du libellé jugé contraignant des lignes directrices. Bien entendu, des lignes directrices ne peuvent servir à établir de nouvelles normes juridiques. Mais nous estimons que notre rôle comme organisme de réglementation consiste notamment à donner une orientation qui clarifie les principes de la LPRPDE et définit les attentes quant à la manière d'interpréter et d'appliquer la loi de façon générale.

En raison du libellé très général de la LPRPDE, les personnes et les organisations ont besoin d'un niveau de certitude adéquat concernant ce qu'implique la conformité. Il est inquiétant que certaines organisations aient manifesté un intérêt à contester la légalité de cette approche. Voilà une autre raison pour laquelle une réforme législative s'impose, car le pouvoir de rendre des ordonnances nous aiderait grandement à faire face à de telles contestations. Signalons que le ministre de l'ISDE a reconnu dans sa réponse au Comité ETHI « qu'il faudra peut-être formuler des lignes directrices ou des règlements plus précis » afin de clarifier les principes de la LPRPDE « pour des modèles ou des produits opérationnels nouveaux ou émergents ».

Pour en savoir plus sur la manière dont la rétroaction des intervenants a été intégrée dans les versions définitives des documents d'orientation, consultez notre site Web.

Réputation

En janvier, le Commissariat a publié les résultats d'une consultation publique sur des questions importantes ayant trait à la réputation et à la vie privée en ligne.

En abordant ce travail, nous avions un objectif clé à l'esprit : aider à créer un environnement en ligne où les gens pourront se servir d'Internet pour explorer leurs intérêts et se développer comme personnes sans craindre que leur trace numérique n'entraîne un traitement injuste.

La nature de l'information a changé radicalement à l'ère numérique, créant par le fait même de nouveaux risques d'atteinte à la réputation des personnes. Les médias sociaux et les moteurs de recherche facilitent grandement l'accès à l'information. Ainsi, des millions de personnes peuvent avoir facilement accès à des renseignements à notre sujet qui pourraient être imprécis, périmés depuis des années ou présentés hors contexte.

Pourtant, on prend à notre égard des décisions importantes à partir de recherches effectuées sur des plateformes de médias sociaux ou au moyen de moteurs de recherche, par exemple des décisions concernant l'emploi, le logement ou le crédit. Les conséquences sont donc réelles.

Il y a lieu de se poser des questions. En tant que société, pensons-nous que la réputation mérite d'être protégée contre les nouveaux risques que posent les renseignements en ligne? Si la réponse est « oui », quelle forme cette protection devrait-elle prendre?

Nous avons examiné divers mécanismes visant à permettre aux personnes d'exercer un certain contrôle sur leurs renseignements en ligne. Nous avons cherché des options propres à établir un équilibre entre le droit à la vie privée et d'autres droits essentiels comme la liberté d'expression et la liberté de la presse.

Il me semble de plus en plus évident que nous devons modifier notre approche en tant qu'organisme de réglementation pour mieux protéger le droit à la vie privée d'un plus grand nombre de Canadiens.

Nous en sommes venus à déterminer que la meilleure façon de procéder était d'interpréter la LPRPDE d'une manière qui protège la réputation en ligne des personnes. D'après nous, en vertu des lois en vigueur, les Canadiens ont le droit de demander aux moteurs de recherche de déréférencer des pages Web et aux sites Web de supprimer ou de modifier un contenu qui renferme des renseignements inexacts, incomplets ou périmés.

Notre projet de position sur la réputation en ligne a également souligné la nécessité de sensibiliser les jeunes Canadiens à l'importance de devenir des citoyens en ligne responsables et bien informés.

Au cours des mois suivant la publication de notre projet de position, nous avons mené d'autres consultations auprès des intervenants.

Entre-temps, le Commissariat a continué de recevoir des plaintes concernant les résultats de recherches sur Google. En réponse, Google a fait valoir que la LPRPDE ne s'appliquait pas à son moteur de recherche et que, en revanche, la désindexation serait inconstitutionnelle si la Loi s'appliquait. Nous avons donc déposé un renvoi devant la Cour fédérale afin d'obtenir des éclaircissements à savoir si le moteur de recherche de Google est assujetti à la LPRPDE avant de procéder plus avant avec les plaintes.

Nous avons également demandé au gouvernement de modifier la loi pour protéger efficacement la réputation des individus dans un monde de plus en plus virtuel. Nous notons avec satisfaction que dans sa réponse au rapport publié par le Comité ETHI en février, le gouvernement a reconnu qu'il faut rendre plus certaine la façon d'appliquer la Loi dans divers contextes où il peut y avoir atteinte à la réputation des personnes.

Une vision proactive de la protection de la vie privée

Il me semble de plus en plus évident que nous devons modifier notre approche en tant qu'organisme de réglementation pour mieux protéger le droit à la vie privée d'un plus grand nombre de Canadiens.

À cette fin, nous avons apporté à notre structure organisationnelle des changements importants qui devraient nous aider à mieux protéger la vie privée.

Nous avons rationalisé nos opérations en clarifiant les fonctions des programmes et simplifiant les relations hiérarchiques. Nous nous sommes davantage tournés vers l'avenir en donnant une plus grande importance aux activités proactives. Notre objectif est d'avoir une incidence plus vaste et plus positive sur le droit à la vie privée d'un grand nombre de Canadiens. Or, ce n'est pas toujours possible lorsque nous accordons presque toute notre attention aux enquêtes sur les plaintes individuelles.

C'est pourquoi nous répartirons dorénavant notre travail entre deux secteurs de programmes : la promotion et la conformité. Les activités visant à amener les ministères et les organisations à se conformer à la loi relèveront du Programme de promotion, tandis que celles visant à régler les problèmes de conformité existants relèveront du Programme de conformité.

Même si nous continuons de chercher à faire renforcer nos pouvoirs d'application de la loi, nous estimons qu'un organisme de réglementation efficace ne privilégie pas d'emblée l'application de la loi et qu'il exerce ces pouvoirs uniquement au besoin. Par conséquent, notre première stratégie se rattachera au Programme de promotion. Elle consistera à informer les Canadiens de leurs droits et de la façon de les exercer, et à travailler auprès des organisations en les guidant sur la façon de s'acquitter de leurs obligations en matière de protection de la vie privée.

Nous donnerons des orientations et de l'information sur la plupart des enjeux clés touchant la vie privée. Nous commencerons par la manière d'obtenir

un consentement valable dans l'environnement numérique complexe d'aujourd'hui ainsi que par les pratiques inacceptables du traitement des données, comme nous l'avons déjà mentionné.

Nous souhaitons aussi travailler de manière proactive et en collaboration avec l'industrie en jouant un rôle consultatif, dans la mesure où nos ressources limitées nous le permettront. Nous voulons mieux comprendre les répercussions des nouvelles technologies sur la vie privée et donner des conseils pratiques concernant la façon d'utiliser ces technologies dans le respect de la vie privée.

Par exemple, nous avons annoncé en mai 2018 notre premier projet consultatif qui porte sur Sidewalk Toronto, initiative de ville intelligente menée conjointement par Waterfront Toronto et Sidewalk Labs, qui appartient à Alphabet, société mère de Google. Le projet vise à bâtir un quartier axé sur la technologie dans le secteur riverain de l'est de la ville. Il utilise des capteurs qui aideront les urbanistes à réaliser des gains d'efficience.

Naturellement, ce projet soulève de nombreuses questions concernant la collecte de données, la protection de la vie privée, le stockage des données et leur utilisation possible.

Des membres de la Direction des services-conseils à l'entreprise du Commissariat et des collègues du Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario ont rencontré les promoteurs du projet pour en savoir plus à ce sujet et connaître les mesures qu'ils prennent pour répondre à certaines préoccupations en matière de protection de la vie privée.

Nous leur avons rappelé les principes clés de la protection de la vie privée, notamment la détermination des fins de la collecte, l'obtention du consentement, l'accès des intéressés à leurs renseignements personnels et les responsabilités de la protection des données et des indications claires quant à savoir à qui ces données appartiennent.

Dans l'ensemble, nous sommes encouragés par les efforts que déploie Sidewalk Toronto pour prendre activement en compte la vie privée et les données dans la conception et la mise en œuvre du projet. Comme le projet en est encore à ses débuts, nous continuerons de suivre de près les progrès réalisés et de collaborer de façon proactive avec les représentants de Sidewalk Toronto. Nous espérons aussi que nos conseils seront utiles lorsque d'autres initiatives de ville intelligente verront le jour dans tout le pays.

Nous préférons aborder d'emblée les questions de protection de la vie privée et les régler dans un esprit de collaboration plutôt que d'avoir recours à des mesures officielles d'application de la loi. Nous éviterons ainsi des enquêtes longues et coûteuses et aiderons à atténuer tout risque futur d'atteinte à la vie privée, tout en offrant aux organisations une certaine uniformité et une certaine prévisibilité dans leurs interactions avec le Commissariat et en permettant à tous de tirer parti de l'innovation.

Voilà pourquoi nous envisagerons d'abord d'utiliser nos outils de promotion avant d'employer notre deuxième stratégie : l'application proactive de la loi.

Dans le cadre du Programme de conformité, nos mesures d'application proactive de la loi cibleront les questions de vie privée systémiques, chroniques ou propres à un secteur qui ne sont pas traitées au moyen de notre système de plaintes et qui nous semblent susceptibles de porter gravement atteinte à la vie privée des Canadiens.

Par exemple, nous avons lancé en mai 2018 dans le cadre de ce programme notre première enquête proactive à l'initiative du commissaire. Cette enquête portait sur les pratiques de six courtiers en données et en listes.

Dans le contexte de cette enquête, nous examinons la responsabilité, l'ouverture et la transparence dans la gestion des renseignements personnels, de même que les modes d'obtention du consentement à la collecte, à l'utilisation ou à la communication des

renseignements personnels. Selon nous, ce type d'enquête pourra être bénéfique pour cette industrie et, pour leur part, les consommateurs canadiens l'accueilleront favorablement.

En délimitant nos activités plus clairement entre les deux programmes – la promotion et la conformité –, en étant plus proactifs et en veillant à ce que nos activités soient centrées sur le citoyen, nous espérons que les Canadiens pourront commencer à sentir qu'ils ont plus de pouvoirs et exercent un meilleur contrôle sur leurs renseignements personnels – et généralement à se sentir plus en sécurité en sachant que leurs droits seront respectés.

Par ailleurs, le mandat de la Direction des services-conseils au gouvernement consiste également à formuler des avis, dans son cas aux institutions fédérales, ce que nous nous sommes engagés à faire plus souvent. Nous souhaitons collaborer avec les fonctionnaires concernés dès le début de l'élaboration des programmes et des activités afin que les Canadiens puissent profiter des avantages de l'innovation sans que leur vie privée soit menacée. À cette fin, nous améliorerons nos lignes directrices sur les évaluations des facteurs relatifs à la vie privée et faciliterons la tâche des institutions qui les mènent.

Bien entendu, la portée de notre programme proactif dépendra des ressources à notre disposition. Nous avons fait des efforts considérables pour gagner en efficacité et faire une utilisation optimale de nos ressources et de nos outils. Néanmoins, nous sommes incapables de suivre le rythme des défis que représente l'environnement numérique de plus en plus complexe dans lequel nous vivons, en grande partie parce que les lois canadiennes sur la protection des renseignements personnels ne sont pas adaptées aux réalités du 21e siècle.

Nous avons demandé une augmentation modeste du financement permanent à titre de mesure provisoire en attendant la réforme législative bien nécessaire. Si nous les recevions, ces fonds aideraient :

- à élaborer un programme proactif limité visant entre autres à donner aux organisations une meilleure orientation stratégique sur les nouveaux enjeux et à renseigner les Canadiens de manière à ce qu'ils puissent exercer un contrôle sur leurs renseignements personnels;
- à gérer la déclaration obligatoire des atteintes, responsabilité qui entrera en vigueur en novembre et qui, comme ce fût le cas ailleurs, devrait augmenter considérablement notre charge de travail, sans que le Commissariat ait reçu de financement connexe comme c'est le cas ailleurs;
- à aider nos enquêteurs submergés de travail à traiter plus rapidement les plaintes déposées par les Canadiens inquiets et à faire enquête de façon proactive sur les enjeux liés à la protection de la vie privée qui sont systémiques, persistants et propres à un secteur.

Par suite de l'affaire Facebook et Cambridge Analytica, le Comité ETHI nous a demandé de quels outils et ressources le Commissariat pourrait avoir besoin pour l'aider à s'assurer que les géants de la technologie et les autres entreprises respectent véritablement leurs obligations en matière de protection de la vie privée.

Alors qu'une augmentation modeste de notre budget aurait un impact intéressant mais limité, un budget beaucoup plus élevé pourrait être nécessaire afin d'apporter une véritable amélioration au respect de la vie privée des Canadiens, tel qu'envisagé par le Comité ETHI. C'est d'ailleurs la conclusion à laquelle en est récemment venu le gouvernement du Royaume-Uni, qui a décidé de doubler les ressources à la disposition de mon homologue du Commissariat à l'information britannique. Un tel financement permettrait de doter le Commissariat à la protection de la vie privée du Canada d'une série complète d'outils de promotion et de conformité adéquats.

Un financement intégral permettrait de produire une gamme complète de documents d'orientation et de s'assurer qu'ils restent à jour. C'est essentiel lorsque les avancées technologiques créent chaque jour de nouveaux risques d'atteinte à la vie privée.

Ce financement nous permettrait de donner des conseils à un plus grand nombre d'organisations désireuses d'utiliser les nouvelles technologies d'une manière qui respecte la vie privée. Nous avons déjà constaté un vif intérêt pour une prestation accrue de services-conseils aux entreprises par le Commissariat; à l'heure actuelle, cependant, notre programme de conseils limité est nettement insuffisant pour répondre à la demande exprimée.

Afin d'améliorer le contrôle exercé par les Canadiens sur leurs renseignements personnels, nous pourrions utiliser des moyens novateurs, par exemple de la publicité contextuelle, pour attirer les gens sur notre site lorsqu'ils sont sur le point de décider de communiquer ou non leurs renseignements personnels.

Nous mettrions également au point des stratégies efficaces avec des organismes de réglementation d'autres domaines afin que les entreprises se conforment à l'ensemble des lois applicables, qui parfois se chevauchent. Enfin, un financement intégral permettrait au Commissariat d'être à la fois proactif dans ses enquêtes et de répondre en temps utile aux plaintes présentées par les citoyens, assurant ainsi un meilleur respect de la vie privée.

Mot de la fin

En résumé, les récents événements mettent en lumière les risques considérables d'atteinte à la vie privée à l'ère numérique. Si nous voulons offrir aux Canadiens la protection à laquelle ils s'attendent – et ont droit –, il est urgent d'adopter des lois modernes qui cadrent avec les normes internationales en pleine évolution.

Nous avons lancé plusieurs initiatives dans le cadre de nos compétences actuelles afin de renforcer cette protection. Toutefois, pour être un organisme de réglementation véritablement efficace, il nous faut de nouveaux pouvoirs et de nouvelles ressources.

En juin dernier, le vice-président du Comité ETHI, Nathaniel Erskine-Smith, a déposé un projet de loi d'initiative parlementaire visant à habiliter le Commissariat à effectuer des vérifications, à rendre des ordonnances et à renvoyer aux fins de poursuite pénale les cas d'infraction délibérée ou irréfléchie à la loi, qui pourraient être passibles d'amendes.

Les récents événements mettent en lumière les risques considérables d'atteinte à la vie privée à l'ère numérique. Si nous voulons offrir aux Canadiens la protection à laquelle ils s'attendent – et ont droit –, il est urgent d'adopter des lois modernes qui cadrent avec les normes internationales en pleine évolution.

À mon avis, le gouvernement aurait dû depuis longtemps déposer un projet de loi en ce sens, et il devrait le faire sans délai, quoique le projet en cause pourrait être bonifié en remplaçant le recours au droit criminel par un régime de sanctions administratives pécuniaires. Je note que l'attribution de nouveaux pouvoirs au Commissariat est une mesure qui a reçu l'appui de tous les partis au sein du Comité ETHI.

En attendant la conclusion de sa consultation sur l'élaboration d'une stratégie de protection des données et l'adoption d'une législation ayant une plus grande portée, nous demandons aussi au gouvernement d'augmenter nos ressources afin que le Commissariat dispose des outils nécessaires pour protéger adéquatement la vie privée des Canadiens.

La protection de la vie privée en chiffres

297	Plaintes en vertu de la LPRPDE acceptées*
205	Plaintes en vertu de la LPRPDE fermées par règlement rapide*
106	Plaintes en vertu de la LPRPDE fermées à l'issue d'une enquête ordinaire*
116	Déclarations d'atteinte à la sécurité des données en vertu de la LPRPDE
1 254	Plaintes en vertu de la LPRP acceptées*
441	Plaintes en vertu de la LPRP fermées par règlement rapide*
767	Plaintes en vertu de la LPRP fermées à l'issue d'une enquête ordinaire*
286	Déclarations d'atteinte à la sécurité des données en vertu de la LPRP
71	Évaluations des facteurs relatifs à la vie privée (EFVP) reçues
50	Avis donnés à des organisations du secteur public à la suite de l'examen d'une EFVP ou d'une consultation à cet égard
571	Communications de renseignements dans l'intérêt public par les institutions fédérales
31	Lois et projets de loi examinés sous l'angle de leurs répercussions sur la vie privée
14	Comparutions devant des comités parlementaires sur des questions touchant les secteurs privé et public
20	Mémoires officiels présentés au Parlement sur des questions touchant les secteurs privé et public
11	Autres interactions avec des parlementaires ou leur personnel (par exemple correspondance avec le bureau de députés ou de sénateurs)
10 092	Demandes d'information
79	Allocutions et présentations
2 095 447	Consultations du site Web
200 840	Consultations du blogue
989	Gazouillis envoyés
13 976	Abonnés sur Twitter au 31 mars 2018
55 010	Publications diffusées
64	Annonces et communiqués diffusés

* Comprend une plainte représentative pour chaque série de plaintes connexes. Pour en savoir plus, consultez l'annexe 2 – Tableaux statistiques.

Loi sur la protection des renseignements personnels et les documents électroniques

Rétrospective de l'exercice

CONSENTEMENT ET CONTRÔLE

Notre rapport sur le consentement était la pièce maîtresse du Rapport annuel au Parlement 2016-2017. Nous y examinions attentivement l'obligation d'obtenir un consentement valable pour recueillir, utiliser et communiquer des renseignements personnels, comme la LPRPDE l'impose aux organisations.

À l'ère de l'analyse des données, de l'intelligence artificielle, de la robotique, du profilage génétique et de l'Internet des objets, nous avons reconnu que la pierre angulaire de la loi fédérale sur la protection des renseignements personnels dans le secteur privé au Canada, c'est-à-dire le consentement, était mise à rude épreuve. Nous avons néanmoins conclu que le consentement demeure essentiel à l'autonomie personnelle et qu'il devrait continuer de jouer un rôle important dans la protection de la vie privée lorsqu'il peut être donné de manière valable en toute connaissance de cause.

Toutefois, comme nous l'indiquions, le consentement doit être appuyé par d'autres mécanismes si nous voulons protéger la vie privée efficacement, notamment des organismes de réglementation indépendants qui renseignent les citoyens, guident l'industrie et l'obligent à rendre des comptes et imposent des sanctions en cas de conduite inappropriée.

À cette fin, plusieurs activités que nous avons menées au cours de l'exercice écoulé visaient directement à renforcer le consentement et le contrôle sous le régime de la LPRPDE.

Orientation en matière de consentement

Peu après le dépôt de notre Rapport annuel 2016-2017, nous avons publié des versions provisoires de nos *Lignes directrices pour l'obtention d'un consentement valable* et de notre *Document d'orientation sur les pratiques inacceptables*. Ces thèmes figuraient en tête d'une liste de 30 sujets de discussion dans le rapport sur le consentement de l'an dernier. Nous avions alors indiqué que nous commencerions à diffuser de l'information et des orientations nouvelles ou mises à jour dans la mesure où nos ressources limitées nous permettraient de le faire.

Nous avons encouragé les intervenants à nous faire part de leur opinion et nous avons reçu 13 mémoires déposés principalement par des associations représentant des entreprises.

Après avoir examiné ces mémoires, nous avons modifié nos lignes directrices et notre document d'orientation et publié les versions définitives en mai 2018. Le Document d'orientation sur les pratiques inacceptables du traitement des données à l'intention des entreprises est entré en vigueur le 1er juillet.

Nos Lignes directrices pour l'obtention d'un consentement valable donnent des conseils pratiques et réalistes aux organisations. Pour sa part, le document d'orientation fait état de zones interdites. Il établit ainsi des limites qui protègent les personnes contre les pratiques inacceptables des entreprises en matière de traitement des données.

Pour de plus amples renseignements sur la réponse du Commissariat aux commentaires reçus des intervenants en ce qui a trait au document d'orientation préliminaire, y compris des précisions sur certains changements apportés ou non aux versions définitives, veuillez consulter le document suivant :

Commentaires du Commissariat à la protection des renseignements personnels sur la rétroaction reçue pendant la consultation de 2017 sur l'orientation en matière de consentement

On trouve aussi dans les lignes directrices d'autres conseils importants concernant le consentement, dont sept principes directeurs. Nous y soulignons quatre éléments sur lesquels il faut mettre l'accent dans les avis de confidentialité et qu'il faut expliquer de manière conviviale :

- les renseignements personnels qui seront recueillis;
- les tiers auxquels les renseignements personnels seront communiqués;
- les fins auxquelles les renseignements personnels seront recueillis, utilisés ou communiqués;
- le risque de préjudice et d'autres conséquences pouvant être causés par la collecte, l'utilisation ou la communication de renseignements personnels.

Certains intervenants ont exprimé des préoccupations concernant notre décision d'intégrer le risque de préjudice parmi ces éléments. Cette décision découle de la définition de « consentement valable », selon laquelle la personne doit comprendre non seulement la nature et les fins, mais également les *conséquences* éventuelles de la collecte, de l'utilisation ou de la communication des renseignements personnels auxquelles elle a consenti.

Nous parlons ici des risques résiduels qui pourraient subsister malgré tous les efforts déployés par une organisation pour prendre des mesures d'atténuation afin de réduire les risques et les répercussions de préjudices éventuels. L'avis doit mentionner uniquement les risques résiduels importants de préjudice grave. On entend par « risque important » un risque qui se situe en deçà de la prépondérance des probabilités, mais qui est supérieur à une possibilité minimale ou à une simple possibilité.

Le terme « préjudice grave » est défini au paragraphe 10.1(7) de la LPRPDE. Il vise notamment :

- la lésion corporelle;
- l'humiliation;
- le dommage à la réputation ou aux relations;
- la perte de possibilités d'emploi, d'occasions d'affaires ou d'activités professionnelles;
- la perte financière, le vol d'identité et l'effet négatif sur le dossier de crédit;
- le dommage aux biens ou leur perte.

Certains ont aussi exprimé des préoccupations concernant le libellé jugé contraignant de la version préliminaire des lignes directrices. Il est clair que nous ne pouvons pas nous servir de lignes directrices pour établir de nouvelles normes juridiques, mais nous estimons que notre rôle à titre d'organisme de réglementation consiste notamment à donner des orientations qui clarifient les principes généraux énoncés dans la LPRPDE et définissent les attentes quant à la façon dont on devrait généralement interpréter la loi. En raison du libellé très général de la LPRPDE, ce type d'orientation aide à donner aux personnes et aux organisations un certain degré de certitude quant à l'application de la loi.

Ainsi, dans la version définitive des lignes directrices, nous faisons la distinction entre, d'une part, les exigences et, d'autre part, les pratiques exemplaires ou les recommandations. Il s'agit d'un changement important et utile que nous avaient recommandé des intervenants. En bref, nous avons ajouté une liste de contrôle qui établit une distinction entre ce qui « doit » être fait (que nous considérons comme une exigence juridique) et ce qui « devrait » être fait (que nous considérons comme une pratique exemplaire).

En ce qui concerne le nouveau document d'orientation sur les pratiques inacceptables, le contexte est de toute évidence important dans l'application du paragraphe 5(3) de la LPRPDE, mais nous sommes convaincus qu'il est utile, voire nécessaire, de citer des exemples particuliers de pratiques généralement jugées inacceptables. Ces précisions devraient établir des limites utiles pour les personnes et les organisations.

Nos *Lignes directrices pour l'obtention d'un consentement valable*, qui ont été publiées en collaboration avec les commissariats de l'Alberta et de la Colombie-Britannique, n'entreront en vigueur qu'en janvier 2019. Les organisations auront ainsi le temps voulu pour apporter les changements nécessaires à leurs systèmes et pratiques. Le document d'orientation du Commissariat sur les pratiques inacceptables est en vigueur depuis le 1er juillet 2018.

Réputation

En 2015, le Commissariat a fait de la réputation et de la protection de la vie privée l'une de ses quatre priorités stratégiques liées à la vie privée. En raison de la prolifération des médias sociaux et des nouvelles technologies de communication, nous nous inquiétions de la facilité avec laquelle les gens peuvent publier des renseignements sur eux-mêmes ou d'autres personnes et de la difficulté de supprimer ou de modifier ces renseignements une fois qu'ils ont été publiés en ligne.

Par exemple, un adulte pourrait avoir l'impression que sa réputation est entachée par les opinions controversées qu'il a exprimées et publiées en ligne à l'adolescence. Mentionnons également la publication en ligne d'un contenu diffamatoire, par exemple dans un blogue; de photos d'un mineur qui, plus tard, portent atteinte à sa réputation; de photos intimes; ou de renseignements concernant la religion d'une personne, sa santé mentale ou d'autres éléments de nature très sensible.

Notre objectif était d'aider à créer un environnement en ligne où les gens peuvent se servir d'Internet

pour explorer leurs intérêts et se développer comme personnes sans craindre que leur trace numérique n'entraîne un traitement injuste.

Le Commissariat a lancé une consultation et un appel de mémoires portant sur la réputation en ligne. À la lumière des mémoires reçus et de notre propre analyse, nous avons publié en janvier un projet de position sur la réputation en ligne qui préconise des solutions permettant de trouver un équilibre entre la liberté d'expression, l'intérêt public et les intérêts des personnes en matière de protection de la vie privée.

Le Commissariat a conclu dans son rapport préliminaire que les Canadiens ont le droit en vertu de la LPRPDE de demander aux responsables des moteurs de recherche de déréférencer des pages Web et à ceux des sites Web de supprimer ou de modifier le contenu renfermant des renseignements inexacts, incomplets ou périmés. Cette proposition établit des parallèles avec le principe du « droit à l'oubli » existant au sein de l'Union européenne.

Nous avons aussi réclamé :

- l'amélioration des mesures de protection pour les enfants et les jeunes lorsqu'ils atteignent l'âge de la majorité;
- l'intégration de la protection de la vie privée aux programmes d'éducation visant l'acquisition de connaissances numériques dans l'ensemble du pays pour aider à former des citoyens en ligne responsables et bien informés;
- l'étude de cet enjeu dans son ensemble par le Parlement.

Tout en reconnaissant que le déréférencement ne constitue pas nécessairement une solution parfaite pour protéger la réputation, nous estimons qu'il s'agit néanmoins d'un outil important à notre disposition sous le régime de la loi actuelle. Toutefois, étant donné les droits concurrents associés à cet enjeu, nous sommes d'avis que cette solution mérite de faire l'objet d'un examen approfondi par les élus.

Dans son rapport sur la réforme de la LPRPDE, le Comité ETHI a étudié attentivement cet enjeu. Il a conclu que le gouvernement devrait modifier la LPRPDE afin d'y ajouter un cadre pour un droit au déréférencement et à la suppression de contenu Web fondé sur le modèle de l'Union européenne. Le Comité a convenu qu'un renforcement des mesures de protection reposant sur le déréférencement et l'effacement de données s'impose pour les adolescents à tout le moins.

Pendant ce temps, le Commissariat a continué de recevoir des plaintes concernant les résultats de recherches sur Google. En réponse à l'une de ces plaintes, Google a affirmé que, contrairement à ce qu'indique le Commissariat dans son projet de position, la LPRPDE ne s'applique pas à son service de moteur de recherche, et que si la LPRPDE exigeait la désindexation de contenu public licite, cela serait inconstitutionnel..

Afin d'obtenir des éclaircissements à savoir si la LPRPDE s'applique au moteur de recherche de Google, nous avons déposé un renvoi devant la Cour fédérale afin qu'elle détermine si le service de moteur de recherche de Google recueille, utilise ou communique des renseignements personnels dans le cadre d'activités commerciales et est donc assujetti à la LPRPDE, et si Google est exempté des dispositions de la Loi parce qu'il a une fonction exclusivement journalistique ou littéraire. Notre document de position demeurera sous forme préliminaire et les plaintes reçues resteront en suspens jusqu'à ce que la Cour rende sa décision concernant l'applicabilité de la LPRPDE.

De plus, dans le contexte de la réputation en ligne, l'arrêt de la Cour suprême du Canada dans *Google inc. c. Equustek Solutions inc.* (2017) est digne de mention. Dans cette affaire, la Cour a conclu qu'un tribunal

canadien peut accorder une injonction interlocutoire mondiale contre un moteur de recherche pour faire retirer des sites Web des résultats de recherche. Cette affaire portait sur un litige commercial, mais elle a des conséquences sur la vie privée qui pourraient se répercuter dans le débat sur le « droit à l'oubli ». Pour en savoir plus sur cette affaire, consultez la section Dossiers relatifs à la protection de la vie privée devant les tribunaux dans le présent rapport.

Examen de la LPRPDE

À l'issue de son examen de la LPRPDE, le Comité ETHI a publié en février 2018 son rapport intitulé Vers la protection de la vie privée dès la conception : Examen de la *Loi sur la protection des renseignements personnels et les documents électroniques*. Notre rapport sur le consentement, initialement publié dans notre Rapport annuel au Parlement de 2016-2017, faisait partie des éléments pris en compte par le Comité.

Le Commissariat a eu plusieurs occasions de présenter ses observations sur la réforme de la LPRPDE avant la publication du rapport.

Nous avons réclamé le pouvoir de rendre des ordonnances et d'imposer des sanctions administratives pécuniaires afin de forcer les entreprises qui ne le feraient pas autrement à respecter la loi. Dans nos mémoires, nous avons insisté sur le fait que des sanctions seraient imposées dans le but de promouvoir la conformité, et non de punir, et qu'elles serviraient d'incitatif important pour les organisations, tout en soulignant que ces pouvoirs nous permettraient de combler un retard face à plusieurs de nos homologues à l'échelle internationale.

Nous avons également demandé de nouveaux pouvoirs pour mener des examens de la conformité, sans qu'il y ait nécessairement eu infraction à la LPRPDE. Ces pouvoirs nous permettraient d'aborder de manière plus proactive les enjeux liés à la protection de la vie privée peu susceptibles de donner lieu à une plainte puisqu'ils font intervenir des modèles opérationnels complexes ou des flux de données opaques dont très peu de Canadiens sont conscients.

À ce sujet, nous avons réclamé plus de souplesse pour ce qui est de choisir les plaintes sur lesquelles faire enquête afin de mieux utiliser nos ressources limitées. De plus, dans les cas où nous refuserions de faire enquête, nous avons demandé que les personnes puissent exercer un recours judiciaire à déterminer, par exemple un droit privé d'action.

Le Comité a conclu qu'il est manifestement nécessaire de conférer au Commissariat des pouvoirs supplémentaires en matière d'application de la loi et il a pris au sérieux nos préoccupations concernant le consentement et la réputation. C'est fort encourageant. Dans certains cas, le Comité est allé au-delà de nos recommandations concernant la réforme : il a demandé que le législateur modifie la LPRPDE dans le but de l'harmoniser avec le *Règlement général sur la protection des données* de l'Union européenne, qui est entré en vigueur en mai.

À titre d'exemple, le Comité a demandé de faire de la « protection de la vie privée dès la conception » un élément central de la loi et de l'ajouter aux principes fondamentaux que doivent respecter les organisations. Il a aussi recommandé de prévoir dans la loi un droit à la portabilité des données. Le concept de la protection de la vie privée dès la conception, expression que l'on doit à l'ancienne commissaire à l'information et à la protection de la vie privée de l'Ontario, préconise la protection de la vie privée dès l'étape de conception de tout nouveau produit ou service.

Dans nos observations, nous avons également souligné l'importance de maintenir le caractère adéquat de la loi canadienne au regard de la législation de l'Union européenne. Depuis 2001, la libre circulation des données est autorisée entre l'Union européenne et le

Canada. En raison de l'entrée en vigueur du *Règlement général sur la protection des données* (RGPD) – nouvel instrument européen de protection des données –, les autorités européennes examineront tous les quatre ans les décisions relatives au caractère adéquat des lois sur la protection de la vie privée d'un pays quant à leur capacité d'offrir aux citoyens européens une protection équivalente à celle dont ils bénéficient en Europe.

Le Comité a été à l'écoute de nos préoccupations. Il a demandé au gouvernement de prendre des mesures appropriées pour assurer le maintien de l'échange de données sans heurts entre le Canada et l'Union européenne.

Les allégations du printemps dernier concernant Facebook et Cambridge Analytica, cabinet-conseil, ont propulsé les enjeux de protection de la vie privée sur le devant de la scène internationale. Le Commissariat et d'autres organismes de réglementation font enquête sur cette affaire, mettant en cause la collecte de données personnelles de millions d'utilisateurs de Facebook à leur insu dans le but d'influencer leur opinion politique.

Non seulement cet incident a ouvert les yeux de bien des gens en montrant que le temps de l'autoréglementation est terminé, mais aussi il a mis en évidence le manque de surveillance exercée sur les pratiques de traitement des renseignements personnels des partis politiques. Cette lacune importante, en partie, a incité le gouvernement du Canada à déposer le projet de loi C-76. Toutefois, ce projet de loi est bien en deçà des normes internationales et n'ajoute rien d'important en matière de protection de la vie privée. Il nous faut faire beaucoup plus pour régir l'utilisation des renseignements personnels par les partis politiques si l'on veut que la vie privée des Canadiens soit protégée de manière adéquate.

À la suite de cet incident, le Comité ETHI a examiné les répercussions sur la vie privée des monopoles de plateformes. Il s'est aussi penché sur des solutions possibles pour assurer la confidentialité des renseignements personnels des citoyens et l'intégrité des processus démocratiques et électoraux dans le monde. Le Commissariat a participé à cet examen. En juin, le Comité a publié son rapport provisoire intitulé Aborder les vulnérabilités de la vie privée numérique et les menaces potentielles au processus électoral démocratique canadien. En plus d'exhorter le gouvernement à prendre des mesures pour s'assurer que les lois sur la protection des renseignements personnels s'appliquent aux activités politiques, il a réitéré la nécessité de renforcer les pouvoirs d'application de la loi conférés au Commissariat. Le Comité a indiqué qu'« on ne peut trop insister sur l'urgence de la situation ».

Par ailleurs, le gouvernement a présenté sa réponse au rapport sur la réforme de la LPRPDE publié en février par le Comité. Il est encourageant de constater que le gouvernement convient de la nécessité de modifier les lois canadiennes sur la protection des renseignements personnels, mais nous sommes déçus que ces changements ne se matérialiseront vraisemblablement pas avant plusieurs années, après la tenue des consultations sur le numérique et les données et après les élections fédérales de l'automne 2019.

Nous demandons au gouvernement d'appliquer immédiatement les recommandations du Comité qui visent à renforcer les outils d'application de la loi à notre disposition. C'est une idée largement soutenue par les parlementaires, les Canadiens et les intervenants du domaine de la protection de la vie privée.

En plus de contribuer à l'examen de la LPRPDE par le Comité, le Commissariat a participé à d'autres examens parlementaires portant à la base sur les questions du consentement et du contrôle exercé par les individus sur leurs renseignements personnels.

Nous avons notamment donné des conseils au Comité permanent de l'industrie, des sciences et

de la technologie de la Chambre des communes concernant la Loi canadienne anti-pourriel ainsi qu'au Comité sénatorial permanent des transports et des communications concernant les véhicules branchés et automatisés. Pour en savoir plus, consultez notre section sur les comparutions devant le Parlement.

Sommaire des principales enquêtes liées au consentement et au contrôle

Microsoft : Donner aux utilisateurs de Windows 10 voix au chapitre concernant l'information qu'ils fournissent

Le Commissariat a ouvert en 2016 une enquête sur une plainte concernant les paramètres de confidentialité par défaut du système d'exploitation Windows 10 de Microsoft. Nous voulions savoir si, pendant le processus d'installation de Windows 10, les utilisateurs avaient la possibilité de consentir en toute connaissance de cause à la collecte et à l'utilisation de leurs renseignements personnels par Microsoft.

Microsoft a collaboré avec le Commissariat en apportant des changements pour appliquer les recommandations issues de notre enquête. Cela dit, Microsoft est l'une des entreprises les plus grandes et les plus influentes dans le monde. Plus d'un milliard de personnes à l'échelle mondiale utilisent son système d'exploitation Windows. Nous étions donc étonnés que Microsoft n'ait pas cerné et pris en compte de manière proactive, avant le lancement de Windows 10, les nombreuses préoccupations en matière de protection des renseignements personnels qui ont fini par être soulevées au cours de l'enquête du Commissariat et par d'autres organismes de protection des données ailleurs dans le monde.

Pendant notre enquête, Microsoft a lancé deux mises à jour de Windows 10. La plus récente, appelée « Creators Update », comprenait cinq paramètres de confidentialité nouveaux ou mis à jour (la localisation, les diagnostics, les expériences personnalisées, les publicités pertinentes et la reconnaissance vocale). Par défaut, ces cinq paramètres étaient réglés à « activé » et « complet » pendant l'installation de la mise à jour. Pour chacun de ces paramètres, nous avions soulevé des préoccupations quant à savoir si Microsoft fournissait aux utilisateurs l'information nécessaire pour prendre une décision éclairée en matière de consentement.

Pour le paramètre de localisation, par exemple, nous avons recommandé à Microsoft de préciser clairement qu'une application tierce pouvait déterminer l'emplacement d'un utilisateur même lorsque cette fonction était désactivée. Nous lui avons demandé de prendre des mesures pour atténuer ce risque. De plus, nous avons recommandé à Microsoft de régler par défaut le paramètre de la collecte de données de diagnostic sur l'ordinateur de l'utilisateur à l'option « de base » plutôt que « complet ». Enfin, nous lui avons également demandé d'établir un protocole officiel documenté pour s'assurer que les données de diagnostic sensibles recueillies auprès des utilisateurs ne serviront pas à offrir des « expériences personnalisées ».

En ce qui concerne les « publicités pertinentes », nous avons recommandé à Microsoft de préciser que ce paramètre ne s'applique pas au consentement de l'utilisateur aux pratiques de publicité pertinentes de Microsoft même et d'ajouter un énoncé dirigeant les utilisateurs vers un mécanisme distinct leur permettant d'indiquer s'ils veulent recevoir des « publicités personnalisées » et, le cas échéant, de choisir lesquelles. En outre, pour ce qui est de la « reconnaissance vocale », nous avons recommandé que Microsoft permette aux utilisateurs d'activer cette option, plutôt que de les forcer à la désactiver, et que l'entreprise supprime toutes les données recueillies qui vont à l'encontre des choix des utilisateurs concernant la reconnaissance vocale.

Dans sa réponse, Microsoft s'est engagée à apporter plusieurs changements pour répondre à nos préoccupations. En premier lieu, il n'y a plus

d'options présélectionnées pour les paramètres de confidentialité au cours de l'installation de Windows 10. Les utilisateurs ont maintenant le choix d'activer les paramètres de confidentialité comme ils le veulent au lieu d'avoir à désactiver ceux qui leur sont proposés. Il s'agit là d'une très bonne chose. Ce changement donne un exemple positif aux autres entreprises qui veulent obtenir un consentement en ligne aux paramètres de confidentialité.

Microsoft s'est également engagée :

- à améliorer ses communications sur la protection de la vie privée;
- à renforcer ses procédures de confidentialité;
- à corriger et à supprimer toutes les données recueillies qui vont à l'encontre des choix de l'utilisateur concernant la reconnaissance vocale;
- à mettre en place des mesures pour atténuer les risques associés aux applications de tiers pouvant déterminer l'emplacement exact d'un utilisateur lorsque le paramètre « localisation » est désactivé.

Dans le cadre de notre évaluation de la mise à jour « Creators Update », nous avons travaillé en étroite collaboration avec nos homologues des Pays-Bas. À la lumière des conclusions et des recommandations découlant de leur enquête et de celles d'autres organisations, Microsoft a apporté plusieurs changements à la version européenne du système d'exploitation.

La version canadienne de Windows 10 est quelque peu différente, mais les changements apportés par Microsoft à son pendant européen sont pertinents et complémentaires aux conclusions de notre évaluation du système d'exploitation. Par exemple, Microsoft a fait en sorte que tous les paramètres doivent être activés conformément à notre recommandation selon laquelle les utilisateurs doivent consentir explicitement à l'envoi à Microsoft de tout renseignement autre que les données de diagnostic de base concernant leur ordinateur.

Consultez le rapport de conclusions d'enquête portant sur Microsoft.

Facebook : L'entreprise accepte de ne plus utiliser des renseignements personnels de non-utilisateurs figurant dans le carnet d'adresses des utilisateurs

En juin 2013, Facebook a avisé le Commissariat d'une atteinte à la sécurité de données téléchargées par les utilisateurs de Facebook au moyen de l'outil d'importation des contacts. Quelques jours plus tard, nous avons reçu une plainte d'une personne alléguant que l'entreprise avait recueilli et communiqué les renseignements personnels d'utilisateurs et de nonutilisateurs de Facebook sans leur consentement.

Pour mettre les faits en contexte, l'outil d'importation des contacts de Facebook, aussi connu sous le nom « Retrouver des amis », permet aux utilisateurs de télécharger et de stocker les coordonnées de leurs contacts dans leur compte Facebook. Par la suite, Facebook utilise ces renseignements pour proposer des personnes avec qui les utilisateurs pourraient vouloir devenir amis. Cette fonction permet aussi aux utilisateurs d'envoyer des courriels pour inviter leurs contacts non utilisateurs à s'inscrire et à se créer un compte Facebook.

En 2012, des ingénieurs de Facebook ont élaboré un processus qui associe avec la même personne diverses coordonnées téléchargées par différents utilisateurs. Par exemple, deux utilisateurs peuvent avoir dans leur carnet d'adresses un contact en commun ayant le même numéro de téléphone, mais une adresse de courriel différente. En associant les différentes coordonnées téléchargées par plusieurs utilisateurs, Facebook peut déterminer avec plus d'exactitude si un contact dont les coordonnées ont été téléchargées par un utilisateur a déjà un compte Facebook. Cette fonction évite d'envoyer un courriel à l'utilisateur pour l'inviter à se créer un compte Facebook.

À peu près à la même période en 2012, un autre groupe d'ingénieurs de Facebook a ajouté à l'outil « Télécharger vos renseignements » une nouvelle fonction permettant aux utilisateurs de télécharger une copie de tous leurs contacts importés. Toutefois, l'outil téléchargeait trop de renseignements – selon Facebook, il s'agirait d'une erreur de codage.

Pour chacun des contacts d'un utilisateur, l'outil téléchargeait également tous les renseignements recueillis à partir du carnet d'adresses d'autres utilisateurs et les associait au contact en question. Par conséquent, d'après Facebook, les coordonnées supplémentaires de près de six millions d'utilisateurs partout dans le monde ont été communiquées, dont celles de quelque 142 000 utilisateurs au Canada.

De plus, environ 14 millions de coordonnées (adresses de courriel et numéros de téléphone) ne pouvant être associées à aucun utilisateur de Facebook ont également été communiquées en raison de cette atteinte à la sécurité des renseignements personnels. Facebook affirme n'avoir reçu aucune plainte concernant cette utilisation abusive de données et n'avoir détecté ni sur son site ni dans l'outil de téléchargement des renseignements aucun comportement inhabituel qui porterait à croire que les personnes touchées à la suite de l'erreur de codage ont été victimes d'actes répréhensibles ou qu'elles ont subi un préjudice.

En collaboration avec le commissaire à la protection des données de l'Irlande, nous avons ouvert une enquête coordonnée portant sur plusieurs questions soulevées à la suite de cette atteinte. Le but était notamment de savoir si Facebook obtient un consentement valable des utilisateurs et des non-utilisateurs pour utiliser leurs renseignements personnels dans le cadre du processus d'association.

Nous n'avons relevé aucun problème touchant la façon dont le média social s'y prend pour permettre aux utilisateurs de télécharger leurs contacts dans leur compte Facebook. Toutefois, nous avons conclu que le processus d'association des carnets d'adresses constitue une utilisation des renseignements personnels d'utilisateurs et de non-utilisateurs pour laquelle Facebook doit obtenir un consentement valable. Les divers avis transmis par Facebook aux utilisateurs ne décrivent pas clairement le processus d'association ni son fonctionnement. En particulier, ces avis n'expliquent pas comment les diverses coordonnées des utilisateurs, notamment celles importées par d'autres utilisateurs, seront utilisées dans le cadre du processus d'association de carnets d'adresses.

Facebook a contesté ces conclusions en faisant valoir qu'elle transmettait à ses utilisateurs des avis à plusieurs niveaux concernant la collecte et l'utilisation des renseignements personnels pour les fonctions d'invitation et de suggestion d'amis. Elle a en outre affirmé que les utilisateurs s'inscrivent à la plateforme dans le but de communiquer avec des amis et qu'ils comprennent que son but même est d'aider les gens à communiquer.

Pour donner un consentement éclairé, il faut comprendre les fins, la nature et les conséquences de la collecte, de l'utilisation et de la communication des renseignements personnels. Dans le cas en question, l'utilisation des coordonnées par Facebook vise à améliorer un service de base consistant à permettre aux gens de communiquer sur son réseau social. Après avoir examiné les observations de Facebook, nous avons convenu que, dans ce cas précis, l'entreprise n'a pas modifié les fins de l'utilisation des coordonnées des utilisateurs de Facebook. En fait, elle utilise simplement les coordonnées autrement que par le passé pour atteindre les mêmes fins. Dans les circonstances, un utilisateur s'attendrait tout de même généralement à ce que les coordonnées servent à suggérer des amis. Nous avons donc conclu que la plainte concernant le consentement n'était pas fondée.

Par ailleurs, nous n'étions pas convaincus que Facebook faisait preuve de suffisamment de transparence en ce qui a trait au traitement des coordonnées, en particulier lorsqu'elle expliquait la

façon dont les contacts téléchargés seraient utilisés pour aider la personne et les autres à retrouver des amis. Facebook n'explique pas ce qu'elle entend par « autres ». Dans ce cas, nous avons conclu que le langage utilisé n'était pas clair et n'expliquait pas convenablement le processus d'association – c'est-à-dire que Facebook combine et associe les coordonnées d'un utilisateur avec les renseignements téléchargés par d'autres utilisateurs.

Facebook a indiqué que, tout en contestant respectueusement les conclusions du Commissariat sur cet enjeu, elle révisera l'avis concernant l'outil d'importation des contacts et le processus d'association. Par conséquent, le Commissariat a déterminé que la plainte faisant état d'une préoccupation à l'égard de la transparence était fondée et conditionnellement résolue.

À la suite de la publication des conclusions de notre enquête, Facebook nous a transmis les avis modifiés expliquant le processus d'association qui sont affichés sur les pages de renseignements supplémentaires de l'outil d'importation des contacts, les pages d'aide et la page portant sur la gestion des contacts téléchargés ainsi que dans la Politique d'utilisation des données. Le Commissariat croit que les avis modifiés expliquent maintenant clairement le processus d'association utilisé par Facebook pour permettre aux personnes de communiquer sur le réseau social.

Il y avait également la question des renseignements personnels de non-utilisateurs qui sont téléchargés par les utilisateurs lorsqu'ils importent leurs contacts dans Facebook et que Facebook utilise pour son processus d'association. L'entreprise a fait valoir que, lorsqu'elle envoie un courriel à un non-utilisateur pour l'inviter à créer un compte Facebook, elle explique l'utilisation prévue de ses renseignements. Encore une fois, nous avons jugé que l'avis n'explique pas vraiment le fonctionnement du processus d'association. De plus, nous avons constaté que Facebook utilise déjà les renseignements personnels des non-utilisateurs sans leur consentement pour leur envoyer un courriel.

Sans moyen réaliste d'obtenir le consentement des non-utilisateurs, Facebook a suivi notre recommandation et ne conserve plus les coordonnées des non-utilisateurs qui ont été associées. L'entreprise a indiqué que le processus d'association des carnets d'adresses n'englobait plus les cordonnées non associées avec un utilisateur actuel de Facebook, ce qui signifie qu'elle ne conserve plus les coordonnées des non-utilisateurs qui ont été associées. Par conséquent, le Commissariat a conclu que la plainte était fondée et résolue.

Pour les besoins de notre enquête, nous avons aussi collaboré avec Facebook pour nous assurer que les utilisateurs ont accès à tous les renseignements ayant été associés à eux et qu'ils peuvent les corriger. Une solution à court terme élaborée par Facebook permet aux utilisateurs d'avoir accès à ces données et de les corriger. Par conséquent, nous avons jugé que cette plainte était fondée et résolue.

Facebook s'est également engagée à concevoir une solution à long terme pour rectifier la situation dans le cadre des efforts qu'elle déploie pour se conformer au *Règlement général sur la protection des données*. Nous continuerons de collaborer avec l'entreprise afin de l'aider à élaborer une solution à long terme pour les utilisateurs.

Consultez le rapport de conclusions d'enquête portant sur Facebook.

Profile Technology : Une entreprise a enfreint la *Loi sur la protection de la vie privée* en réutilisant des millions de profils d'utilisateurs canadiens de Facebook

Nous avons reçu des plaintes de plusieurs personnes alléguant que leurs renseignements personnels avaient été recueillis dans d'anciens profils et groupes Facebook et utilisés sans leur consentement pour créer de nouveaux profils sur un autre site de réseautage social appelé « Profile Engine » (www.profileengine.com).

Les plaignants affirmaient avoir découvert par hasard que leurs renseignements étaient affichés sur le site Profile Engine en faisant des recherches Internet pour voir ce qu'ils pouvaient trouver à leur sujet. Dans un cas, la plaignante nous a indiqué que les renseignements affichés sur le site étaient tirés d'un profil Facebook qu'elle avait à l'adolescence. Elle a précisé que quiconque faisait des recherches à partir de son nom – notamment des employeurs potentiels – présumerait qu'elle manque beaucoup de maturité. Un autre plaignant a affirmé que les allégations de voies de fait qui avaient initialement été publiées sur Facebook avant d'y être supprimées continuaient de s'afficher sur le site.

L'intimée, Profile Technology ltée, a fait valoir que le Commissariat n'avait pas compétence pour faire enquête et publier un rapport sur la plainte puisque l'entreprise était fondée en Nouvelle-Zélande et n'avait aucune présence au Canada. Nous n'avons pas accepté ces arguments. À notre avis, plusieurs facteurs indiquaient un lien réel et substantiel entre les activités de Profile Technology et le Canada, notamment l'affirmation de l'entreprise elle-même selon laquelle son site Web contenait près de 4,5 millions de profils canadiens. Le Commissariat avait donc compétence pour faire enquête sur les plaintes.

Quoi qu'il en soit, Profile Technology a indiqué que son site n'était qu'un moteur de recherche permettant aux gens de trouver des renseignements auxquels le public avait déjà accès dans Facebook, si bien qu'aucun consentement n'était nécessaire. Nous avons conclu que Profile Technology avait peut-être initialement recueilli le profil d'utilisateurs de Facebook afin d'offrir une fonction de recherche aux utilisateurs du réseau social, mais qu'elle avait ensuite copié et utilisé ces renseignements à de nouvelles fins, c'est-à-dire pour établir son propre site de réseautage social.

D'après nous, cette exception au consentement ne s'applique pas puisque le public n'avait pas accès aux profils faisant l'objet des plaintes au sens du règlement d'application de la LPRPDE. Entre autres, nous avons considéré que les profils Facebook sont dynamiques, contrairement à une publication – par exemple un magazine, un livre ou un journal – et que les utilisateurs exercent un contrôle sur leurs renseignements qui y figurent. Au fil du temps, les utilisateurs peuvent mettre à jour et modifier leurs renseignements, bloquer l'accès du public au profil ou supprimer entièrement leur profil. À notre avis, traiter un profil Facebook comme s'il s'agissait d'une publication irait à l'encontre de l'intention de la Loi et porterait atteinte au contrôle que les utilisateurs exercent autrement sur leurs renseignements à la source.

Nous avons constaté que tous les renseignements tirés des profils et des groupes de Facebook faisant l'objet des plaintes avaient été supprimés ou modifiés dans Facebook. En d'autres mots, les renseignements se trouvaient toujours sur Internet uniquement parce qu'ils étaient affichés sur le site Web de Profile Technology. Les profils recueillis et réutilisés par Profile Technology représentaient un instantané dans le temps. L'entreprise avait tout simplement copié les profils pour les afficher sur son propre site en les laissant tels quels.

Nous avons conclu que Profile Technology n'avait pas obtenu le consentement des intéressés pour utiliser leurs renseignements personnels de cette façon. Il était évident à nos yeux qu'une personne raisonnable ne considérerait pas l'utilisation des renseignements sur le site de Profile Technology comme appropriée dans les circonstances. Nous avons recommandé à Profile Technology de supprimer tous les profils et les groupes associés à des Canadiens, notamment ceux associés aux plaignants.

Profile Technology a carrément refusé d'appliquer notre recommandation. Le mépris flagrant de l'entreprise à l'égard des obligations en matière de protection des renseignements personnels ainsi que son entêtement tout au long de l'enquête – elle

transmettait souvent des réponses superficielles à nos demandes d'information ou n'y répondait pas – ont eu pour effet de prolonger l'enquête sur cette affaire complexe.

Avant la publication de notre rapport d'enquête, l'entreprise a supprimé tous les profils de son site Web. Les moteurs de recherche ne pouvaient plus référencer les renseignements, ce qui a éliminé un élément clé des plaintes. Toutefois, Profile Technology a téléchargé une grande partie de ces renseignements sur Internet (d'abord sur Internet Archive). Les renseignements ont été téléchargés dans des fichiers de base de données distinctes et certains identificateurs ont été supprimés ou chiffrés. Ainsi, les renseignements sont facilement accessibles dans ce format pour le téléchargement par partage de poste à poste, y compris sur le Web caché.

Par conséquent, nous n'avons aucun moyen de savoir comment les données téléchargées par Profile Technology sur Internet peuvent être utilisées et diffusées à l'avenir dans la mesure où n'importe qui peut les télécharger, recréer les fichiers et exploiter les renseignements à ses propres fins. Par exemple, l'exploitant d'un site Web pourrait afficher les renseignements et imposer des frais aux personnes pour les supprimer ou les renseignements pourraient servir à porter atteinte à la réputation des gens.

Dans le but d'atténuer ces types de risques, nous avons communiqué avec le Commissariat à la protection de la vie privée de la Nouvelle-Zélande pour lui faire part de nos conclusions et discuter de nos préoccupations. Celui-ci a accepté d'examiner notre rapport et de se pencher sur les options à sa disposition sous le régime de la loi néo-zélandaise sur la protection de la vie privée. Il vérifiera également si d'autres lois du pays pourraient s'appliquer. Nous continuerons de collaborer avec nos homologues de la Nouvelle-Zélande dans toute la mesure permise en vertu de la LPRPDE afin d'appuyer toute nouvelle mesure dans ce dossier.

Nous avons aussi communiqué avec Facebook pour déterminer si elle pourrait nous renseigner sur les fichiers de base de données affichés sur Internet par Profile Technology. Facebook a confirmé être au courant de la situation et précisé qu'elle explorait diverses options concernant les renseignements stockés dans Profile Engine, notamment des recours judiciaires relativement à un règlement reconnu par la cour.

Consultez le rapport de conclusions d'enquête portant sur Profile Technology.

Public Executions : Fermeture d'un site Web humiliant les débiteurs

Le Commissariat a reçu plusieurs plaintes au sujet du site Web publicexecutions.com. Moyennant certains frais, ceux qui voulaient recouvrer une créance confirmée par une ordonnance d'un tribunal pouvaient afficher sur le site les détails du jugement. En plus du nom du débiteur et de la somme due, les créanciers et toute autre personne pouvaient afficher des commentaires non vérifiés ainsi que d'autres renseignements personnels sur le débiteur, notamment son adresse, des photos de lui ou la marque de son véhicule. Il était possible d'effectuer une recherche par nom. D'ailleurs, les données sur les plaignants affichées sur le site figuraient parmi les principaux résultats d'une recherche effectuée au moyen d'un moteur de recherche à partir de leur nom.

Les plaignants alléguaient que le propriétaire du site Web portait atteinte à leur droit à la vie privée en vertu de la LPRPDE, car il y publiait des renseignements personnels les concernant sans leur consentement dans le but de les humilier pour les obliger à payer leurs dettes.

Le propriétaire du site Web a fait valoir que la LPRPDE ne s'appliquait pas, puisqu'il n'y avait aucune relation vendeur-consommateur avec les débiteurs, et que la publication des renseignements personnels des individus n'était pas liée à une activité commerciale. Il a par ailleurs soutenu que son site Web pratiquait une forme de journalisme, raison supplémentaire l'exemptant des exigences de la LPRPDE relatives au consentement.

La communication des renseignements personnels d'un individu par un tiers moyennant certains frais est de toute évidence une activité commerciale, si bien que la LPRPDE s'applique. De plus, nous n'avons rien trouvé à l'appui de l'affirmation selon laquelle le site pratiquerait une forme de journalisme. Selon un récent jugement de la Cour fédérale (*A. T. c. Globe24h*), une activité devrait être qualifiée de journalistique uniquement lorsqu'elle concerne un « élément de la production originale ». Or, il n'y avait rien d'original dans les renseignements stockés sur le site Web, qui ne servait qu'à afficher des renseignements fournis par d'autres.

Dans ses conclusions, le Commissariat a pris en compte la décision du ministère des Services gouvernementaux et des Services aux consommateurs de l'Ontario selon laquelle le site Web exerçait ses activités illégalement en tant qu'« agence de renseignements sur le consommateur » non inscrite au sens de la *Loi sur les renseignements concernant le consommateur* de l'Ontario. Ainsi, l'utilisation et la communication de renseignements concernant les dettes des individus étaient rigoureusement réglementées en vertu de cette loi.

Dans cette affaire, le site Web communiquait des renseignements personnels à grande échelle. Le Commissariat a donc conclu que, contrairement aux exigences du paragraphe 5(3) de la LPRPDE, une personne raisonnable n'estimerait pas acceptable qu'une organisation publie ces renseignements à grande échelle pour réaliser un gain financier et contraindre les débiteurs à payer leurs dettes, alors qu'il existe des mécanismes juridiques permettant d'exécuter les jugements.

Le propriétaire a rejeté notre recommandation de supprimer de son site Web tous les renseignements relatifs aux débiteurs et de prendre des mesures pour les faire supprimer des mémoires caches des moteurs de recherche.

Nous avons conclu que les plaintes étaient fondées. Comme nous n'avons pas le pouvoir d'ordonner au propriétaire de supprimer tous les renseignements sur son site Web, les plaintes n'ont pu être réglées. Nous avons donc dû exercer le pouvoir que nous confère la LPRPDE et intenter une action en justice devant la Cour fédérale du Canada afin d'obliger le propriétaire à appliquer nos recommandations.

C'est uniquement après que la poursuite eut été intentée que le propriétaire a avisé le Commissariat qu'il avait fermé son site Web et qu'il n'avait pas l'intention de le rétablir. Par conséquent, le Commissariat a abandonné sa demande auprès de la Cour. Il continuera toutefois de surveiller la situation pour s'assurer que le site Web n'est pas rétabli sous une forme quelconque.

Consultez le rapport de conclusions d'enquête portant sur Public Executions.

Entreprise de messagerie : L'entreprise met fin à sa politique de livraison chez un voisin à la suite d'une plainte pour absence de consentement

Dans ce dossier, la plaignante alléguait qu'une entreprise de messagerie avait communiqué ses renseignements personnels sans son consentement en livrant chez son voisin un colis qui lui était adressé. Le colis, que la plaignante ne s'attendait pas à recevoir, provenait d'une institution financière et contenait des renseignements financiers sensibles.

L'entreprise a expliqué avoir pour politique de livrer le colis chez un voisin ou de le laisser à un point de ramassage lorsque la signature du destinataire était exigée et que celui-ci n'était pas à la maison. Elle a précisé que l'option de livraison chez un voisin était offerte parce que de nombreux clients préféraient ne pas avoir à se rendre à un point de ramassage pour prendre possession de leur colis. L'entreprise a ajouté obtenir auprès de l'expéditeur le consentement à la livraison chez un voisin.

D'après les modalités d'expédition de l'entreprise, en l'absence du destinataire, un colis pour lequel une signature était exigée pouvait être livré chez un voisin.

Toutefois, on ne sait pas au juste si l'entreprise de messagerie s'attendait à ce que l'expéditeur obtienne le consentement du destinataire pour livrer un colis à un voisin.

Nous avons communiqué avec l'institution financière de la plaignante, qui nous a affirmé avoir compris que le destinataire devrait se rendre au point de ramassage s'il n'était pas disponible pour signer l'accusé de réception. L'institution financière a indiqué ne pas savoir qu'il s'agissait d'une pratique courante de demander à un voisin d'accuser réception d'un colis.

Nous avons conclu que l'entreprise de messagerie n'avait pas obtenu le consentement de la plaignante pour demander à un voisin d'accuser réception du colis en son nom. Nous avons également conclu qu'elle n'indiquait pas clairement aux expéditeurs quand et comment un colis pourrait être laissé chez un voisin et que ceuxci devraient obtenir le consentement du destinataire en pareil cas.

En réponse à notre recommandation préconisant l'obtention d'un consentement valable à l'avenir, l'entreprise a indiqué qu'elle n'offrirait plus l'option de la livraison chez un voisin à compter de juillet 2018. Nous avons jugé que la plainte était fondée et résolue puisque l'entreprise s'était engagée à mettre fin à la pratique en cause. Étant donné que plusieurs entreprises du secteur de la livraison laissent des colis chez un voisin, nous encourageons toutes les entreprises à revoir leurs pratiques pour s'assurer qu'elles sont conformes à la LPRPDE.

Consultez le résumé de conclusions portant sur l'entreprise de messagerie.

ENQUÊTES EN VERTU DE LA LPRPDE EN GÉNÉRAL

Aperçu

Au cours de l'exercice 2017-2018, nous avons accepté 297 plaintes aux fins d'enquête et clos 311 dossiers d'enquête.

- Comme au cours des exercices antérieurs, le secteur des finances a continué à être en cause dans la plupart des plaintes reçues en vertu de la LPRPDE. Il représentant près du quart des enquêtes en vertu de la LPRPDE (24 % ou 74 enquêtes) en 2017-2018.
- Les organisations des secteurs des télécommunications (13 % ou 40 plaintes), d'Internet (10 % ou 32 plaintes) et des services (13 % ou 39 plaintes) ont également fait l'objet d'un grand nombre de plaintes.

ENQUÊTES EN VERTU DE LA LPRPDE 2017-18

297 plaintes acceptées

Le secteur des finances représente près du quart des plaintes

Plus de la moitié des 311 dossiers clos portaient sur des problèmes de consentement (24 %) et d'accès aux renseignements personnels (29 %)

- De plus, poursuivant la tendance des dernières années, les Canadiens ont déposé davantage de plaintes portant sur des problèmes d'accès aux renseignements personnels (29 % ou 86 plaintes) et de consentement (24 % ou 70 plaintes). Ensemble, ces plaintes représentent plus de la moitié de celles reçues en 2017-2018.

Afin de tirer le maximum de nos ressources d'enquête, nous continuons de privilégier le processus de règlement rapide pour fermer efficacement les plaintes peu complexes. En 2017-2018, nous avons clos de cette façon deux tiers (66 %) des plaintes en vertu de la LPRPDE.

Toutefois, malgré tous les efforts déployés pour accroître notre efficacité, nous avons continué à avoir de la difficulté à répondre à la demande d'enquêtes officielles et notre arriéré de dossiers de plus d'un an n'a cessé de croître. D'ailleurs, à la fin de 2017-2018, un tiers de nos enquêtes actives (55) remontaient à plus de 12 mois.

Plusieurs facteurs ont une incidence sur notre capacité à fermer les dossiers d'enquête dans le délai de 12 mois prescrit par la LPRPDE. Il est facile de recueillir, d'utiliser et de communiquer des renseignements personnels et on peut le faire à peu de frais. Cette situation a transformé la réalité de la protection de la vie privée. L'utilisation de mégadonnées, de l'intelligence artificielle et d'autres technologies pour tirer une valeur des données brutes continue de prendre de l'ampleur.

Ces technologies, que l'on pouvait à peine imaginer au moment de l'entrée en vigueur de la LPRPDE, peuvent avoir des répercussions importantes et réelles sur la vie privée des Canadiens. De plus en plus d'enquêtes nécessitent des analyses technologiques approfondies pour évaluer les questions liées à la vie privée, puis formuler des recommandations pertinentes. Notre enquête sur une plainte relative au consentement mettant en cause le système d'exploitation Windows 10 de Microsoft (décrite plus tôt dans le présent rapport) n'est qu'un exemple.

Nos enquêtes sont encore plus complexes en raison de la nécessité de comprendre les modèles d'affaires, que la technologie et la monétisation des données rendent de plus en plus complexes et fluides, et de demeurer au fait de leur évolution.

Parce que notre modèle actuel ne nous permet pas de choisir les plaintes qui méritent une enquête dans les limites de nos ressources, les enquêtes sur ces nouvelles questions complexes se rajoutent à toutes celles sur les autres plaintes qu'il est impossible de fermer par règlement rapide à la satisfaction des plaignants. De plus, comme nous n'avons pas le pouvoir d'ordonner des changements ou d'imposer des sanctions aux organisations en cas de non-conformité, les organisations peuvent tarder à répondre à nos questions dans le cadre de nos enquêtes et à s'engager à prendre des mesures correctives.

Autres enquêtes en vertu de la LPRPDE

Comme le montrent les enquêtes résumées précédemment, la technologie a créé une foule de problèmes concernant le consentement à la collecte et à l'utilisation des renseignements personnels et le contrôle exercé sur ceux-ci. Elle a aussi créé de nouveaux défis en matière de protection des renseignements personnels contre toute communication non autorisée. En vertu de la LPRPDE, les organisations doivent protéger les renseignements qu'elles détiennent au moyen de mesures de sécurité correspondant à leur degré de sensibilité – plus les renseignements sont sensibles, plus le niveau de protection doit être élevé.

La LPRPDE ne précise pas les mesures de sécurité à prendre. Il incombe donc aux organisations de déterminer les outils physiques, technologiques ou organisationnels appropriés qui sont nécessaires pour protéger adéquatement les renseignements personnels.

Toutefois, comme en témoignent les résumés d'enquête présentés ci-après, la sécurité dans le monde numérique ne peut reposer sur un effort ponctuel. Il faut constamment examiner les mesures de sécurité pour s'assurer que les renseignements sensibles sont protégés contre les menaces nouvelles et émergentes.

AMA : L'Agence améliore ses mesures de sécurité déficientes concernant la protection des renseignements personnels des athlètes à la suite d'une enquête sur une atteinte d'envergure mondiale

Comme en fait état le Rapport annuel 2016-2017, le Commissariat a pris connaissance en septembre 2016 d'un accès inapproprié à la base de données de l'Agence mondiale antidopage (AMA). Cette organisation établie à Montréal surveille la conformité à la réglementation antidopage dans les sports amateurs à l'échelle internationale. Plus précisément, un groupe appelé « Fancy Bear » a diffusé sur son propre site Web et ailleurs le nom de certains athlètes ayant participé aux Jeux olympiques de 2016 à Rio ainsi que leurs renseignements personnels qui avaient été extraits du Système d'administration et de gestion antidopage (ADAMS).

Afin de situer l'incident en contexte et d'indiquer le motif probable de cette atteinte, il est important de souligner les événements dramatiques qui s'étaient produits avant les Jeux de Rio. En juillet 2016, l'AMA a publié les résultats d'une enquête indépendante confirmant certaines allégations de manipulation par l'État russe des procédures de contrôle du dopage lors des Jeux olympiques d'hiver de 2014 à Sotchi[1]. Des dénonciateurs russes avaient prétendu que l'État avait participé à une opération de dopage d'envergure en Russie, ce que les autorités russes niaient avec force. Par la suite, les Jeux de Rio se sont déroulés du 5 au 21 août 2016 et 118 athlètes russes ont été exclus des épreuves.

D'après notre enquête, le piratage aurait commencé par une campagne d'hameçonnage : des courriels semblant provenir du dirigeant principal de la technologie de l'AMA ont été envoyés aux employés de l'Agence. Cette tactique a permis de pirater trois comptes de courriel au sein de l'organisation. Par la suite, les pirates ont obtenu l'accès au compte d'un administrateur d'ADAMS et ont alors commencé à s'en servir pour consulter sur une période de plusieurs jours les renseignements stockés dans le système.

La sécurité dans le monde numérique ne peut reposer sur un effort ponctuel. Il faut constamment examiner les mesures de sécurité pour s'assurer que les renseignements sensibles sont protégés contre les menaces nouvelles et émergentes.

Il va sans dire qu'une grande partie des renseignements personnels stockés dans ADAMS sont très sensibles. Il s'agit de renseignements sur la santé, plus précisément sur des troubles médicaux, des médicaments, des ordonnances et des analyses d'échantillons de substances corporelles, voire des renseignements génétiques figurant dans le passeport biologique des athlètes. De plus, ADAMS renferme aussi des renseignements sur les infractions aux règles antidopage et les déplacements des athlètes.

L'atteinte à la sécurité de ces renseignements peut entraîner des préjudices graves et multiples. Ainsi, l'accès à certains renseignements personnels sur la santé et leur communication sans autorisation peuvent causer une stigmatisation, une discrimination et des préjudices psychologiques. La diffusion de résultats d'analyse défavorables qui, pour des raisons légitimes, n'avaient pas été rendus publics peut constituer une source d'embarras et de honte pour les athlètes et nuire grandement à leur réputation, à leur image ainsi qu'à leur vie personnelle et professionnelle.

1 Déclaration de l'AMA: L'Enquête indépendante confirme l'intervention de l'État russe dans les procédures de contrôle du dopage.

Tout cela donne à penser que l'AMA, au moment de concevoir ses mesures de sécurité, doit prendre en compte l'importance des renseignements qu'elle détient aux yeux de ceux qui peuvent chercher à les obtenir par des moyens illégaux. Elle doit aussi envisager la possibilité qu'elle continue d'être la cible de cyberattaques complexes. Selon certains rapports rendus publics, le groupe Fancy Bear est lié à des activités de piratage sous l'influence d'un État.

Au moment de l'atteinte, l'AMA avait mis en place certaines mesures de sécurité de nature technologique, physique et organisationnelle. Or, il y avait de toute évidence d'importantes failles et le niveau de l'environnement de sécurité était bien inférieur à celui que l'on est en droit d'attendre d'une organisation chargée de détenir des renseignements médicaux très sensibles susceptibles de porter gravement atteinte à la réputation et à l'intégrité des athlètes et à l'ensemble du mouvement olympique. L'AMA doit mettre en place un cadre de mesures de sécurité suffisamment robustes, d'autant plus qu'elle constitue une cible de grande valeur pour les pirates informatiques expérimentés, notamment ceux parrainés par un État.

Dans son rapport préliminaire, le Commissariat a recommandé à l'AMA de renforcer ses mesures de sécurité afin d'assurer par plusieurs moyens la sécurité et la confidentialité des renseignements personnels sensibles dont elle a la gestion :

- élaborer un cadre de sécurité de l'information complet comprenant des politiques et des procédures écrites pour contrer les risques;
- mettre en place de mesures de sécurité appropriées relativement aux contrôles d'accès;
- utiliser des protocoles de chiffrement adéquats pour les données sous sa garde stockées dans ADAMS;
- s'assurer que la sécurité des applications et la détection des intrusions sont bien configurées et que les systèmes et les registres font l'objet d'une surveillance active et adéquate.

En réponse au rapport préliminaire du Commissariat, l'AMA a accepté d'appliquer toutes les recommandations. Le Commissariat a donc conclu que la plainte était fondée et conditionnellement résolue. En conséquence, il surveillera étroitement la mise en œuvre de ses recommandations par l'organisation et, à cette fin, il a conclu un accord de conformité avec l'AMA.

VTech : Atteinte massive à la vie privée en raison du défaut d'un manufacturier de jouets d'appliquer des correctifs à des vulnérabilités bien connues

Au début de décembre 2015, VTech Holdings Limited, fabricant de jouets éducatifs électroniques connectés au Web a avisé le Commissariat d'une atteinte mondiale à la sécurité de données. D'après le fabricant, dont le siège social est situé à Hong Kong, cette atteinte pourrait avoir mis en péril les renseignements personnels de plus de 300 000 enfants canadiens – nom, date de naissance, photos, enregistrements vocaux et contenu de séances de clavardage. De plus, VTech a affirmé que les renseignements personnels d'environ 237 000 adultes canadiens, pour la plupart les parents des enfants touchés, pourraient également avoir été mis en péril.

Peu de temps après la réception de cet avis, un Canadien touché par l'atteinte a déposé une plainte auprès du Commissariat. Le plaignant alléguait que VTech n'avait pas protégé adéquatement les renseignements personnels de ses clients en permettant à des pirates informatiques d'avoir accès à leurs renseignements, dont potentiellement les siens et ceux de son fils.

L'enquête, menée en collaboration avec nos homologues à l'étranger, la Federal Trade Commission des États-Unis et le Commissariat à la protection de la vie privée et des données de Hong Kong, a révélé que le pirate avait eu accès à un des réseaux de VTech par injection SQL. Il s'agit d'une faille de sécurité bien connue et largement exploitée.

L'enquête a également révélé qu'entre autres lacunes, VTech ne menait pas d'essais réguliers pour détecter les vulnérabilités et qu'elle n'avait par conséquent pris aucune mesure pour protéger ses réseaux contre ce type de cyberattaque facilement évitable.

VTech a agi rapidement pour atténuer le plus possible l'incidence du piratage en avisant ses clients par courriel et par d'autres moyens et en leur conseillant des mesures à prendre afin de réduire le risque d'atteinte à la sécurité de leurs renseignements personnels. L'entreprise s'est également engagée à mettre en place diverses mesures pour améliorer la sécurité de ses réseaux et protéger les renseignements personnels de ses clients.

En conséquence, nous avons conclu que la plainte était fondée et résolue.

Soulignons que, malgré les vives inquiétudes suscitées par cette atteinte chez les clients de VTech, dont des centaines de milliers de Canadiens, il est possible que très peu de renseignements personnels aient été mis en péril. Le pirate informatique, qui a été arrêté, a affirmé avoir voulu seulement attirer l'attention sur les lacunes des mesures de sécurité en place chez VTech et n'avoir communiqué qu'une petite quantité de renseignements à un journaliste pour montrer à quel point il était facile d'avoir accès aux réseaux de VTech. Les renseignements communiqués ont été restitués à l'entreprise.

Consultez le rapport de conclusions d'enquête portant sur VTech.

Accès et compagnies aériennes

Le Commissariat a également eu l'occasion de faire enquête sur la façon dont les compagnies aériennes traitent les demandes d'accès dans le cadre de deux affaires distinctes portant sur la communication de renseignements personnels à des tiers.

Jet Airways : La LPRPDE ne confère pas au commissaire le pouvoir d'obtenir des documents à l'égard desquels le secret professionnel de l'avocat est invoqué

Deux plaignants ayant un handicap ont été expulsés d'un avion de Jet Airways à la suite d'un désaccord avec un membre de l'équipage concernant le traitement de leurs animaux d'assistance.

Les plaignants, qui réclamaient une indemnité pour un vol manqué, ont demandé à la compagnie aérienne de leur donner accès à tous les renseignements personnels les concernant en ce qui a trait à leur réservation et à l'incident en question. La compagnie aérienne n'ayant pas répondu à leur demande dans le délai prescrit de 30 jours, les plaignants ont envoyé une deuxième requête. Ils ont alors demandé à la compagnie aérienne si elle avait l'intention de respecter les obligations lui incombant en vertu de la LPRPDE et, dans l'affirmative, quand elle le ferait. La réponse reçue d'un avocat représentant Jet Airways se limitait en grande partie à accuser réception de leur demande.

Les plaignants ont déposé une plainte auprès du Commissariat, alléguant que la compagnie aérienne refusait de leur donner accès à leurs renseignements personnels. Entre-temps, un représentant des plaignants a écrit à la compagnie aérienne afin de l'avertir qu'une plainte serait déposée auprès d'autres organismes de réglementation si la demande d'indemnité n'était pas entièrement réglée dans les 30 jours suivants.

Dans le cadre de notre enquête, la compagnie aérienne a indiqué ne pas avoir répondu à la demande initiale

parce que la personne responsable était en congé de maladie. Les organisations doivent répondre aux demandes d'accès à l'information dans les 30 jours, même si elles refusent l'accès. La compagnie aérienne a rejeté notre recommandation de mettre en place un mécanisme pour s'assurer de respecter cette exigence à l'avenir.

Quoi qu'il en soit, la compagnie aérienne a affirmé qu'elle refusait de donner accès aux documents demandés, faisant valoir qu'ils avaient été créés dans le cadre d'un mécanisme officiel de règlement des différends et qu'ils étaient donc visés par une exception en vertu de la LPRPDE. Nous n'avons trouvé aucune preuve d'un processus de règlement officiel des différends établi par la compagnie aérienne, si bien que l'exception ne s'appliquerait pas. L'entreprise s'est dite en désaccord avec cette conclusion.

Jet Airways a également affirmé être justifiée de refuser l'accès aux renseignements puisque les plaignants avaient indiqué qu'ils pourraient déposer une plainte auprès d'un autre organisme de réglementation. D'après la compagnie, comme cet incident pouvait aboutir à des poursuites judiciaires, la loi lui permettait d'invoquer le secret professionnel de l'avocat à l'égard de tout document susceptible d'être utilisé dans le cadre de poursuites à l'avenir.

Le Commissariat n'a pas le pouvoir de contraindre une organisation à fournir les documents pour lui permettre de déterminer s'il est raisonnable d'invoquer le secret professionnel de l'avocat. Dans ce cas, la compagnie aérienne a refusé de communiquer de son plein gré les documents demandés ou de fournir des détails sur la nature des documents en question. Sans voir les documents ou obtenir davantage de détails sur leur contenu, le Commissariat n'a aucun moyen de savoir si l'exception était justifiée et ne peut donc déterminer si l'entreprise était en droit de refuser de communiquer aux plaignants leurs renseignements personnels en invoquant l'exception relative au privilège du secret professionnel de l'avocat.

Cela dit, le Commissariat est convaincu que le secret professionnel de l'avocat invoqué par Jet Airways était beaucoup trop général. La compagnie aérienne a tout d'abord déclaré qu'elle avait pour politique interne de traiter chaque incident en partant du principe qu'il pouvait mener à des poursuites judiciaires. C'est pourquoi tous les documents et les renseignements produits en lien avec l'incident étaient protégés sur la base du privilège.

De l'avis du Commissariat, une politique générale applicable à tous les documents produits à la suite d'incidents survenus à bord d'un appareil ne satisferait pas aux critères justifiant le secret professionnel de l'avocat et le privilège relatif aux litiges. La compagnie aérienne a depuis changé son fusil d'épaule : elle ne soutient plus que tous les documents produits en lien avec un incident survenu à bord d'un appareil sont protégés par le privilège relatif aux litiges. En revanche, à son dire, elle était en droit d'invoquer ce privilège une fois « l'avis juridique » envoyé. D'après le Commissariat, cette ligne de conduite est tout aussi problématique, puisqu'elle pourrait donner lieu à l'invocation du privilège relatif aux litiges pour des documents ayant été produits avant la réception d'un « avis juridique » et principalement dans un but autre que la préparation à un litige.

Le Commissariat a donc conclu que Jet Airways avait contrevenu au principe 4.1.4 en omettant de se doter de politiques et de pratiques donnant effet aux principes de la LPRPDE.

Nous continuons d'encourager la compagnie aérienne à examiner les documents réclamés en vain par les plaignants et à leur transmettre tous les renseignements non protégés par le secret professionnel de l'avocat ou le privilège relatif aux litiges.

Consultez le rapport de conclusions d'enquête portant sur Jet Airways.

Compagnie aérienne : Collecte de renseignements sans consentement et refus d'accès d'une compagnie aérienne autorisés en vertu de la LPRPDE

Après avoir constaté qu'un homme n'avait pas en main les documents requis pour entrer au Canada, les responsables de la sécurité ont avisé la compagnie aérienne avec laquelle il comptait voyager du fait qu'elle devrait lui refuser l'accès à bord de l'appareil. Après que la compagnie aérienne eut refusé sa demande de remboursement, le plaignant lui a demandé de lui donner accès à tous les renseignements personnels le concernant qu'elle avait en sa possession, notamment ceux échangés avec des tiers.

La compagnie aérienne lui a fourni certains documents. Le plaignant, convaincu que d'autres renseignements ne lui avaient pas été communiqués, a déposé une plainte auprès du Commissariat.

La compagnie aérienne a affirmé avoir recueilli des renseignements personnels du plaignant auprès d'une institution fédérale afin d'évaluer sa situation de voyage et communiqué des renseignements le concernant à une institution fédérale qui faisait enquête sur une infraction éventuelle à la ***Loi sur l'immigration et la protection des réfugiés***.

En vertu de la LPRPDE, des renseignements personnels peuvent être recueillis à l'insu de l'intéressé ou sans son consentement si :

- la collecte effectuée au su ou avec le consentement de l'intéressé compromettrait l'exactitude des renseignements ou l'accès à ceux-ci;
- la collecte se fait à des fins liées à une enquête sur la contravention au droit fédéral ou provincial.

Pour ce qui est des renseignements recueillis en vertu de cette exception, l'organisation n'est pas tenue de communiquer à l'intéressé les renseignements le concernant. De plus, en vertu de la LPRPDE, les renseignements personnels peuvent être communiqués à l'insu d'une personne ou sans son consentement par une organisation du secteur privé à une institution fédérale qui fait enquête et recueille des données aux fins du contrôle d'application du droit canadien. De même, lorsqu'il est question des renseignements communiqués en vertu de cette exception, une organisation doit refuser de répondre à la demande d'accès si l'institution fédérale s'y oppose.

En nous basant sur les renseignements obtenus, nous avons jugé que la compagnie aérienne appliquait correctement les exceptions touchant le consentement et l'accès. Nous avons donc conclu que la plainte n'était pas fondée.

Consultez le rapport de conclusions d'enquête portant sur la compagnie aérienne.

Atteintes à la vie privée

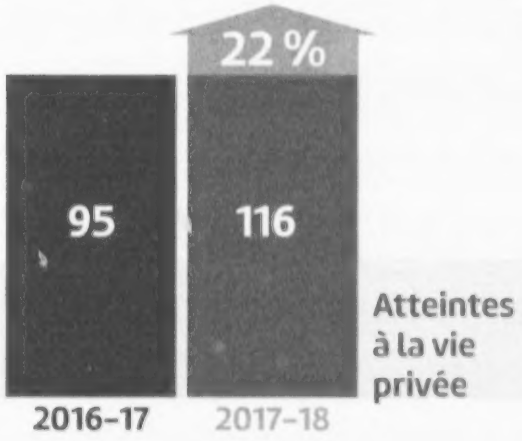
Au cours des dernières années, de nombreuses atteintes notoires à la sécurité des données ont mis en cause des géants de l'industrie au Canada et à l'étranger. Elles ont eu une incidence négative sur les renseignements personnels de Canadiens.

En 2017-2018, nous avons mené à terme des enquêtes portant sur des atteintes de portée mondiale, comme celle concernant l'AMA, et nous en avons ouvert sur certaines cyberatteintes particulièrement importantes dans le secteur privé au Canada à ce jour – par exemple les incidents mettant en cause Bell Canada, Nissan Canada Finance, Uber et l'agence de vérification du crédit Equifax. Ces enquêtes sont en cours et nous communiquerons plus de détails à leur sujet après la fermeture des dossiers de plainte.

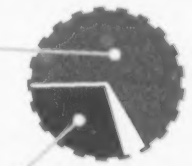
Les atteintes à la sécurité des données, en particulier à la suite de cyberattaques comme celles présentées ci-dessus, peuvent mettre en péril les renseignements personnels de milliers, voire de millions de Canadiens. Ces types d'atteintes se produisent de plus en plus fréquemment et le nombre de cas déclarés au Commissariat a continué d'augmenter en 2017-2018.

En fait, le nombre d'atteintes a doublé depuis 2014, année où le gouvernement a annoncé son intention d'obliger les organisations du secteur privé à déclarer les atteintes.

Cent seize (116) atteintes dans le secteur privé ont été déclarées au Commissariat en 2017-2018, ce qui représente une hausse de 22 % par rapport à l'exercice précédent. Comme par les années passées, les incidents rapportés étaient principalement liés au vol et à l'accès non autorisé (67 %), suivis par la communication accidentelle (29 %).



Le vol des renseignements personnels et l'accès non autorisé à ces renseignements représentent 67 % des atteintes à la vie privée, suivi par la communication accidentelle à 29 %



Bien entendu, il s'agit là des atteintes dont nous avons été informés. Compte tenu du volume considérable de données personnelles recueillies, utilisées et communiquées sur le marché numérique, il y a lieu de croire que de nombreux cas ne sont pas déclarés ni même détectés. À juste titre, les atteintes à la vie privée suscitent des craintes chez les consommateurs et ébranlent leur confiance envers les entreprises avec lesquelles ils font affaire. Au fil du temps, cela peut inspirer de la méfiance à l'égard de l'économie numérique, ce qui n'est dans l'intérêt de personne.

La déclaration obligatoire des atteintes pour le secteur privé entrera en vigueur à l'automne. Elle ne sera assortie d'aucun financement supplémentaire pour le Commissariat. En l'absence de financement correspondant et compte tenu de notre charge de travail déjà lourde, nous ne serons pas en mesure de consacrer le temps nécessaire pour examiner les atteintes et faire enquête comme il se doit. Il s'agit d'une pression parmi d'autres exercées sur nos ressources qui nous ont poussés à demander un financement supplémentaire.

À partir de novembre, la loi obligera les organisations à aviser les personnes touchées de toutes les atteintes qu'elles estiment susceptibles de poser un risque réel de préjudice grave et à déclarer ces atteintes au Commissariat. Le risque sera évalué selon la sensibilité des renseignements visés et la probabilité qu'ils soient mal utilisés. Les organisations doivent aussi tenir un registre des atteintes à la sécurité des données dont elles prennent connaissance et le remettre au Commissariat sur demande.

En avril, Innovation, Sciences et Développement économique Canada a publié le règlement établissant le mode de fonctionnement de l'obligation de déclarer les atteintes et d'en aviser les intéressés.

La publication de ce règlement marque une étape attendue depuis longtemps, à savoir l'entrée en vigueur de la déclaration obligatoire des atteintes à la sécurité des renseignements personnels. Bien que

la déclaration obligatoire constitue un pas vers une meilleure protection des renseignements personnels des Canadiens, le règlement ne va pas assez loin.

Nous sommes d'avis que les déclarations des atteintes devraient fournir au commissaire à la protection de la vie privée les renseignements nécessaires pour qu'il puisse évaluer la qualité des mesures de sécurité des organisations. Sans cette information, nous aurons beaucoup de mal à améliorer les façons de faire en matière de sécurité.

Par ailleurs, nous pourrions utiliser cette information pour compléter celle contenue dans les registres sur les atteintes, ce qui nous permettrait de mieux comprendre les défis associés aux mesures de sécurité et aux atteintes à la protection des données sur le marché. Nous serions ainsi plus à même de conseiller et de guider efficacement les organisations sur la manière d'améliorer leurs mesures de sécurité afin de mieux protéger les renseignements personnels des Canadiens.

Nous sommes aussi d'avis qu'un bon régime de déclarations des atteintes devrait comprendre des sanctions pécuniaires pour les organisations qui en amont, n'ont pas adopté des mesures de sécurité suffisantes, et pas seulement parce qu'elles ont sciemment omis de signaler les atteintes qu'elles ont subies en aval. Sanctionner les organisations qui ont des mesures de sécurité inadéquates serait un moyen de les inciter fortement à prévenir les atteintes, ce qui devrait être l'objectif ultime.

Cela dit, avec les ressources limitées dont nous disposons, nous porterons une attention particulière à la façon dont les organisations corrigent les vulnérabilités en matière de sécurité et évaluent le risque réel de préjudice grave. Nous surveillerons également la façon dont elles tiennent les registres des atteintes. Il s'agit d'une nouvelle obligation imposée par la LPRPDE.

À l'heure actuelle, nous examinons et mettons à jour nos documents d'orientation concernant la déclaration des atteintes afin de prendre en compte la mise en œuvre imminente de la déclaration obligatoire.

ACTIVITÉS PARLEMENTAIRES LIÉES À LA LPRPDE

Comme nous l'avons expliqué en détail dans les sections précédentes, dans le cadre de nos activités parlementaires relatives à la LPRPDE en 2017-2018, nous nous sommes surtout penchés sur les nouveaux enjeux liés au consentement et au contrôle. Parallèlement, dans le cadre de notre mandat, nous avons examiné d'autres initiatives législatives susceptibles d'avoir une incidence sur la protection de la vie privée : nous avons formulé des avis au Parlement au besoin, présenté des mémoires, donné suite à une comparution ou exprimé d'autres points de vue aux comités parlementaires chargés d'étudier ces initiatives.

Entre autres, nous avons :

- participé à l'examen législatif de la Loi canadienne anti-pourriel (LCAP);
- contribué à l'étude du Comité sénatorial des banques et du commerce sur la cybersécurité et la cyberfraude;
- présenté des mémoires au Comité sénatorial des transports et des communications concernant l'incidence possible des véhicules branchés et automatisés sur la vie privée et une proposition de rendre obligatoire les enregistreurs audio-vidéo à bord des locomotives.

Examen prévu par la Loi canadienne anti-pourriel (LCAP)

Dans le cadre de l'examen législatif de la LCAP, le Comité permanent de l'industrie, des sciences et de la technologie de la Chambre des communes a invité le Commissariat à exprimer son point de vue sur le fonctionnement de la loi adoptée il y a trois ans et sur la façon dont on pourrait l'améliorer.

Au cours de sa comparution, le commissaire a affirmé que la LCAP avait eu une incidence positive en aidant à lutter contre les pourriels et à contrer certaines menaces en ligne, notamment les logiciels espions, susceptibles de porter atteinte à la vie privée des Canadiens. Il a également souligné que les dispositions de la LCAP permettant au Commissariat d'échanger des renseignements et de collaborer avec le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) et le Bureau de la concurrence y avaient été pour beaucoup dans le succès de son enquête sur les activités de collecte d'adresses et de pollupostage menées par Compu-Finder.

Parallèlement, le commissaire a fait remarquer que cet échange de renseignements en vertu de la LCAP est limité à certaines circonstances très précises. Il a recommandé de modifier la LCAP ou la LPRPDE pour donner au Commissariat davantage de latitude relativement à l'échange de renseignements avec le CRTC et le Bureau de la concurrence afin de traiter les questions qui touchent à la fois la protection des consommateurs et celle de la vie privée.

Le commissaire a également proposé d'indiquer dans la LCAP que ses dispositions peuvent s'ajouter à celles de la LPRPDE, mais non abaisser les normes de protection. On éviterait ainsi d'autres cas où une organisation tenterait faire valoir qu'elle n'a pas à se conformer à la LPRPDE en raison d'une exception prévue par la LCAP.

Le commissaire a aussi recommandé de modifier la LPRPDE pour indiquer clairement que, si une personne installe un logiciel espion sur un ordinateur, contrevenant ainsi à la LCAP, toute collecte ou utilisation de renseignements recueillis sur cet ordinateur contreviendrait à la LPRPDE.

Dans son rapport, le Comité a recommandé plusieurs modifications à la LCAP, entre autres afin de donner plus de latitude au CRTC pour l'échange de renseignements avec ses partenaires dans l'application de la loi. Dans la réponse du gouvernement au rapport du Comité, le ministre de l'Innovation, des Sciences et du Développement économique a indiqué qu'il était prêt à consulter les organismes chargés de l'application de la LCAP, notamment le Commissariat, avant d'apporter des modifications à la loi.

Étude d'un comité sénatorial sur les véhicules branchés et automatisés

En janvier 2018, le Comité sénatorial des transports et des communications a publié un rapport concernant l'étude sur les questions techniques et réglementaires liées à l'arrivée des véhicules branchés et automatisés.

Le Commissariat a participé à l'étude à deux occasions : le commissaire a comparu devant le Comité en mars 2017 et le Commissariat a présenté un mémoire de suivi en novembre.

Le Commissariat se réjouit du fait que le rapport du Comité fasse écho à plusieurs suggestions et préoccupations qu'il avait formulées. Le Comité a fait plusieurs recommandations axées sur la protection de la vie privée. Il a notamment recommandé que le gouvernement continue d'évaluer la nécessité d'une réglementation en matière de protection des renseignements personnels visant expressément les véhicules branchés et que le Commissariat ait le pouvoir d'enquêter de façon proactive sur le respect de la LPRPDE par l'industrie relativement à ces véhicules et de faire respecter la Loi.

Dans une autre recommandation, nous avons demandé que Transports Canada rassemble divers intervenants pertinents, notamment des gouvernements, des constructeurs automobiles et des consommateurs, afin d'élaborer un cadre pour les véhicules branchés. La protection de la vie privée en est l'un des principaux éléments. Le Commissariat serait heureux de pouvoir participer à l'élaboration du cadre si le gouvernement accepte cette recommandation.

Étude et rapport sur les questions et préoccupations relatives à la cybersécurité et à la cyberfraude

En novembre 2017, le commissaire a comparu devant le Comité sénatorial permanent des banques et du commerce dans le cadre de son étude sur les questions relatives à la cybersécurité et à la cyberfraude.

Entre autres questions, le commissaire a mentionné le règlement imposant la déclaration obligatoire des atteintes à la sécurité des données dans le secteur privé, qui entrera en vigueur en novembre 2018. Il a affirmé que ce règlement constituera un outil important pour améliorer les pratiques de sécurité des organisations, mais que l'on pourrait l'améliorer.

À titre d'exemple, le Commissariat a recommandé que les organisations déclarant les atteintes soient tenues de fournir l'information nécessaire pour évaluer la qualité des mesures de sécurité et de présenter une évaluation du risque de préjudice. D'après le commissaire, cette information est « essentielle » à l'établissement des données de référence nécessaires pour dégager les tendances et régler les questions systémiques, ce qui permettrait d'exercer une surveillance efficace.

Soulignant la disparité importante entre les pratiques des différentes institutions fédérales en matière de déclaration des atteintes, le commissaire a réitéré ses recommandations antérieures concernant la modernisation de la *Loi sur la protection des renseignements personnels*, notamment afin que la déclaration obligatoire des atteintes à la vie privée s'applique aussi à ces institutions.

Le commissaire a également abordé la question du point de convergence entre la sécurité et la protection de la vie privée en citant l'exemple des modifications au projet de loi C-59. Les modifications prévoient que le Centre de la sécurité des télécommunications Canada (CSTC) jouerait un rôle dans l'échange de renseignements sur la cybersécurité avec d'autres organisations. En vertu des modifications proposées, selon le contexte de l'échange, ces renseignements peuvent comprendre une communication privée interceptée.

Tout en reconnaissant la nécessité de recueillir toutes ces données pour surveiller efficacement les réseaux, le commissaire a affirmé qu'il est tout aussi important de veiller à limiter la conservation, l'utilisation et la communication des renseignements personnels ainsi recueillis.

En conclusion, le commissaire a souligné l'importance d'une collaboration plus étroite entre les spécialistes de la cybersécurité et les autorités de protection des données comme le Commissariat pour améliorer les mécanismes de défense de notre cyberinfrastructure et faire de la protection de la vie privée un principe directeur des efforts dans le domaine de la cybersécurité.

Projet de loi C-49, Loi apportant des modifications à la Loi sur les transports au Canada et à d'autres lois

Le projet de loi C-49, important projet de loi omnibus portant sur diverses questions liées au transport, a attiré l'attention du Commissariat en raison d'une disposition obligeant les sociétés ferroviaires à installer des enregistreurs audio-vidéo à bord des locomotives (EAVL) dans tous les trains.

Durant l'étude du projet de loi par le Comité sénatorial permanent des transports et des communications, le commissaire a exprimé le point de vue du Commissariat à plusieurs reprises : il a envoyé une lettre en septembre 2017, a comparu devant le Comité en janvier 2018 et a transmis une lettre de suivi en février 2018.

Les observations du Commissariat portaient sur quatre enjeux :

- Le projet de loi prévoit une exception inhabituelle concernant quatre éléments clés de la LPRPDE : la collecte, l'utilisation, la communication et la conservation.
- Il ne définit pas clairement le rôle que jouera le Commissariat dans les enquêtes portant sur les infractions présumées. Nous craignons que le Commissariat ait de la difficulté à avoir accès aux enregistrements des EAVL afin de déterminer s'ils ont été utilisés d'une manière portant atteinte à la vie privée d'un employé. Nous avons recommandé que le projet de loi confirme que le Commissariat a compétence pour faire enquête sur les plaintes concernant des infractions alléguées à la LPRPDE, notamment pour déterminer si les exceptions à la LPRPDE prévues par la *Loi sur la sécurité ferroviaire* ont été correctement appliquées.
- Nous nous demandions si les employés des sociétés ferroviaires auraient le droit de consulter les renseignements personnels les concernant recueillis par les EAVL, comme le prévoit la LPRPDE.
- Le Commissariat a recommandé au Comité de clarifier la portée du pouvoir de réglementation de manière à empêcher l'adoption de règlements ajoutant de nouvelles fins autorisées pour la collecte, l'utilisation et la communication des données des EAVL.

Dans sa lettre de février, le commissaire a aussi souligné que le Commissariat est rarement consulté à l'étape de la rédaction des projets de loi et qu'il ne l'a pas été dans le cas du projet de loi C-49. Il a réitéré une recommandation antérieure voulant que la *Loi sur la protection des renseignements personnels* exige dorénavant des discussions avec le Commissariat lorsqu'un ministère propose des modifications ayant des répercussions sur la vie privée. Le Commissariat est d'avis que le législateur aurait pu répondre à ses préoccupations plus tôt si on l'avait consulté au sujet de dispositions particulières du projet de loi.

Finalement, Transports Canada s'est engagé à faire appel au Commissariat au cours du processus de réglementation pour s'assurer de répondre à ses préoccupations. Le Commissariat estime que cet engagement constitue un pas dans la bonne direction.

Le commissaire a envoyé une nouvelle lettre au Comité sénatorial afin de lui exprimer sa satisfaction à l'égard de l'engagement du Ministère à répondre aux préoccupations du Commissariat dans la réglementation à venir. La lettre indiquait également que le Commissariat maintenait sa position de principe sur les questions soulevées dans sa présentation, notamment pour ce qui est de l'exception aux exigences de la LPRPDE concernant la collecte, l'utilisation, la communication et la conservation des renseignements personnels.

Consultations menées par Finances Canada

Le Commissariat a également présenté ses mémoires à Finances Canada, notamment concernant les répercussions sur la vie privée des modifications apportées au cadre de surveillance des paiements de détail. Il a aussi exprimé son opinion sur l'orientation du cadre fédéral régissant le secteur financier pour l'avenir.

Le Commissariat a ajouté qu'il soutenait l'innovation, tout en soulignant l'importance de tenir compte des obligations existantes imposées au secteur en matière de protection de la vie privée. En outre,

il a mentionné des considérations concernant de nouveaux enjeux comme le système bancaire ouvert et les technologies financières.

En ce qui touche les technologies financières, le Commissariat a exprimé des préoccupations le printemps dernier au sujet de modifications apportées au projet de loi de mise en œuvre du dernier budget, qui visent à autoriser les institutions financières à communiquer des renseignements personnels à un plus large éventail d'organisations.

Finances Canada a affirmé que les modifications ne réduiraient pas la protection des renseignements personnels, mais le Commissariat est en désaccord. Selon nous, les modifications éliminent des obstacles qui empêchent les institutions financières sous réglementation fédérale d'échanger des renseignements personnels avec des entreprises de technologies financières sans s'assurer que des mesures législatives parallèles ont aussi été adoptées pour protéger la vie privée.

Le Commissariat a déclaré privilégier un renforcement de la LPRPDE pour répondre à ces préoccupations. À son avis, toutes les organisations assujetties à la Loi, et non seulement les institutions financières, devraient être tenues d'obtenir un consentement valable et le Commissariat devrait avoir le pouvoir voulu pour s'assurer que les règles de protection de la vie privée sont respectées, notamment le pouvoir de rendre des ordonnances exécutoires visant les organisations qui ne se conforment pas à la Loi.

Le commissaire a souligné que le Commissariat n'avait pas été consulté au sujet des modifications, si bien que l'organisme peut difficilement dire si le juste équilibre a été atteint. Selon l'information dont il disposait, le commissaire a conclu que le projet de loi favorise une plus grande innovation sans toutefois tenir pleinement compte de l'incidence sur la vie privée. Malgré les préoccupations soulevées par le Commissariat, le projet de loi a été adopté tel quel.

PROGRAMME DES CONTRIBUTIONS

Lancé en 2004 en vertu de la LPRPDE, le Programme des contributions du Commissariat octroie chaque année jusqu'à 500 000 $ à l'appui de travaux de recherche réalisés par des établissements d'enseignement supérieur et des organismes sans but lucratif, notamment des associations de l'industrie, des organisations de consommateurs et de bénévoles, des associations commerciales et des organisations de défense des intérêts. Le Commissariat encourage les demandeurs à proposer des projets qui génèrent de nouvelles idées, approches et connaissances dans le domaine de la protection de la vie privée. Ces projets peuvent aider les organisations à mieux protéger les renseignements personnels et les Canadiens à prendre des décisions plus éclairées concernant la protection de leur vie privée.

Le Commissariat encourage les demandeurs à proposer des projets qui génèrent de nouvelles idées, approches et connaissances dans le domaine de la protection de la vie privée. Ces projets peuvent aider les organisations à mieux protéger les renseignements personnels et les Canadiens à prendre des décisions plus éclairées concernant la protection de leur vie privée.

En 2017-2018, le Commissariat a lancé deux appels de propositions. Il a reçu 49 propositions, dont neuf ont été retenues pour obtenir un financement.

Entre autres, le Commissariat a financé deux projets consacrés aux répercussions du nombre croissant de « jouets intelligents » sur la vie privée. Selon les chercheurs des équipes de projet en question, ces jouets recueillent une grande quantité de renseignements personnels au moyen d'un microphone, d'une caméra et d'autres capteurs et, connectés à Internet, ils présentent souvent des vulnérabilités sur le plan de la sécurité susceptibles de porter atteinte à la vie privée des enfants. Les chercheurs ont constaté que les fabricants de jouets recueillent et analysent largement les données, mais qu'ils fournissent très peu d'information aux consommateurs en ce qui a trait aux renseignements recueillis et à la façon dont ils sont utilisés ou communiqués.

Un autre projet financé dans le cadre du Programme des contributions visait à améliorer la protection de la vie privée des jeunes adultes ayant un trouble du développement. À partir de cette recherche, l'équipe du projet a élaboré divers outils d'apprentissage qui aideront les jeunes Canadiens ayant ce type de trouble, ainsi que leur famille et les organisations leur offrant des services, à détecter et à atténuer les risques d'atteinte à leur vie privée.

Loi sur la protection des renseignements personnels

Rétrospective de l'exercice

SÉCURITÉ NATIONALE

Lorsque le projet de loi C-51, *Loi antiterroriste de 2015*, a été déposé à la Chambre des communes en janvier 2015, le Commissariat, à l'instar de nombreux Canadiens, a affirmé craindre qu'il n'atteigne pas un juste équilibre entre les droits individuels – dont le droit à la vie privée – et la sécurité nationale. Malgré cela, le projet de loi a été adopté tel quel en août 2015.

Depuis, le gouvernement s'est engagé à abroger les éléments problématiques du projet de loi C-51 et à adopter de nouvelles dispositions pour renforcer la reddition de comptes en matière de sécurité nationale et atteindre un meilleur équilibre entre la sécurité collective et les droits et libertés. Le commissaire, de concert avec ses homologues provinciaux et territoriaux, a déposé un mémoire dans le cadre de ce processus en décembre 2016.

Projet de loi C-59

Après cette consultation, le projet de loi C-59, *Loi concernant des questions de sécurité nationale*, a été déposé en juin 2017. Au cours de sa comparution devant le Comité permanent de la sécurité publique et nationale en décembre 2017 ainsi que dans un mémoire et une lettre de suivi adressés au Comité, tous deux en mars 2018, le commissaire a affirmé que le projet de loi constituait un pas dans la bonne direction, mais qu'il continuait de susciter des préoccupations.

Le Commissariat a proposé 11 modifications concernant, entre autres, l'examen et la surveillance, les seuils de communication ainsi que la conservation et la destruction des renseignements personnels. Le gouvernement a accepté la grande majorité de nos recommandations et a pris des mesures pour répondre à bon nombre d'entre elles. Le Commissariat se réjouit de ces développements. Le projet de loi révisé a été adopté par la Chambre des communes en juin, et sera étudié au Sénat à l'automne.

Le Commissariat est satisfait de la proposition, qui figure dans le cadre du projet de loi C-59, visant à créer un nouvel organisme de surveillance composé d'experts (l'Office de surveillance des activités en matière de sécurité nationale et de renseignement

[OSASNR]) investi d'un vaste mandat pour examiner les activités de tous les ministères et organismes chargés de la sécurité nationale. Ce comité s'ajoute au nouveau Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR) en vertu du projet de loi C-22.

Ces deux organismes seront en mesure de se communiquer des renseignements confidentiels et, de façon générale, de collaborer afin de produire des examens éclairés et exhaustifs prenant en compte les considérations des experts et des élus. Des modifications ont également été apportées afin de clarifier le rôle du Commissariat dans la surveillance de la sécurité nationale. La loi confère maintenant au Commissariat la souplesse voulue sur le plan juridique pour échanger des renseignements confidentiels avec l'OSASNR. Malheureusement, ce n'est pas le cas pour ses interactions avec le CPSNR.

En ce qui concerne l'échange d'information entre les institutions fédérales, le projet de loi C-59 prévoit qu'une institution fédérale peut communiquer des renseignements si elle est convaincue que « la communication aidera à l'exercice de la compétence ou des attributions de l'institution fédérale destinataire [...] à l'égard d'activités portant atteinte à la sécurité du Canada ». Il prévoit également que « l'incidence de la communication sur le droit à la vie privée d'une personne sera limitée à ce qui est raisonnablement nécessaire dans les circonstances ».

Ces dispositions comprennent certains aspects du critère de nécessité que le Commissariat a recommandé à maintes reprises. La modification exigeant que les institutions destinataires détruisent ou retournent dès que possible les renseignements personnels qui ne sont pas nécessaires à l'exécution de leur mandat constitue un autre signe de progrès.

Enfin, le Commissariat est satisfait de la modification apportée à la définition de l'expression « information accessible au public », du fait qu'elle exclut les renseignements personnels pour lesquels il existe une attente raisonnable de protection de la vie privée. Le Commissariat a également demandé une modification pour préciser que l'information accessible au public comprend l'information publiée ou diffusée en conformité à la loi et que l'information disponible par abonnement ou par achat a été obtenue ou créée par le vendeur de la même manière.

Le Commissariat est satisfait du nouveau principe ajouté au projet de loi qui répond à ces préoccupations. Le principe exige que les activités du CST, notamment celles liées à la collecte de renseignements personnels accessibles au public, soient réalisées dans le respect de la primauté du droit.

Le Commissariat continue de suivre la progression du projet de loi, actuellement à l'étude au Sénat, et garde espoir que la loi définitive atteindra un bien meilleur équilibre entre la protection de la vie privée et la sécurité nationale que les dispositions actuelles.

LA VIE PRIVÉE À LA FRONTIÈRE

Dans le même ordre d'idées, nous avons également continué d'exprimer des préoccupations au sujet du droit à la vie privée à la frontière, tant au Canada qu'aux États-Unis. En vertu d'un décret du président américain Donald Trump, les mesures de protection des renseignements personnels prévues dans la *Privacy Act* ne s'appliquent pas aux personnes qui ne sont pas des citoyens des États-Unis. Ce décret a donné au Commissariat l'occasion de mettre en lumière d'importantes lacunes quant aux recours que peuvent exercer les Canadiens qui se rendent aux États-Unis. Nous avons analysé ces lacunes en détail dans le Rapport annuel 2016-2017.

Depuis, le Commissariat s'est prononcé sur le projet de loi C-23, qui autorise les agents frontaliers américains à mener des activités de précontrôle, y compris des fouilles en sol canadien. Il a exprimé de

sérieuses réserves concernant l'absence de normes permettant de déterminer quand il est approprié de fouiller un téléphone ou d'autres appareils à la frontière.

Décret présidentiel

Bon nombre de Canadiens ont communiqué avec le Commissariat au début de 2017 pour savoir si le décret présidentiel porterait atteinte à leurs droits lorsqu'ils voyagent aux États-Unis. Le décret ordonne aux organismes gouvernementaux américains de veiller à ce que leurs politiques de protection de la vie privée excluent de la protection offerte par la *Privacy Act* des États-Unis (dans la mesure où les lois applicables le permettent) les personnes qui ne sont pas des citoyens ou des résidents permanents des États-Unis.

Le commissaire a écrit une lettre aux ministres de la Justice, de la Sécurité publique et de la Défense nationale afin d'obtenir des éclaircissements sur les protections qui s'appliquent aux voyageurs et de les exhorter à déterminer si les autorités américaines maintiendraient les mesures de protection de la vie privée prévues par diverses ententes multilatérales et bilatérales.

Il a aussi recommandé que le gouvernement demande aux États-Unis d'ajouter le Canada à la liste des pays désignés en vertu de la *Judicial Redress Act*. Cette loi permet aux voyageurs provenant de 26 pays européens de demander aux tribunaux américains d'examiner certains aspects du droit à la vie privée et de leur accorder des droits de recours.

Après des échanges avec leurs homologues américains, les représentants de Sécurité publique Canada ont informé le Commissariat que les autorités américaines leur avaient affirmé que le décret n'avait pas réduit de façon substantielle la protection de la vie privée des Canadiens.

Le Commissariat croit comprendre que certaines ententes continueraient d'être respectées et que les mécanismes de recours demeureraient en place. Malgré la recommandation du Commissariat et celle du Comité permanent de la sécurité publique et nationale de la Chambre des communes, le gouvernement a refusé de demander aux États-Unis d'ajouter le Canada à la liste figurant dans la *Judicial Redress Act*.

Fouille d'appareils électroniques

En 2017-2018, comme par les années passées, le Commissariat a continué d'examiner les pratiques et de recevoir des plaintes concernant la façon dont les agents frontaliers (tant aux États-Unis qu'au Canada) exigent l'accès au téléphone intelligent et aux autres appareils électroniques des individus. Les parlementaires se sont également penchés sur la question. Au cours de sa comparution devant le Comité ETHI en septembre 2017, le commissaire a souligné que les agents de l'Agence des services frontaliers du Canada (ASFC) continuent de considérer les appareils électroniques personnels comme de simples « biens » aux fins de l'application de la *Loi sur les douanes*.

Ainsi, tout appareil personnel peut faire l'objet d'une fouille à la frontière sans aucun motif d'ordre juridique. Il s'agit manifestement d'une idée dépassée qui ne reflète pas les réalités de la technologie d'aujourd'hui. Le commissaire a fait remarquer que, quoique la politique de l'ASFC soit plus nuancée et indique que les appareils électroniques devraient faire l'objet d'une fouille uniquement lorsque « les appareils ou les supports numériques pourraient contenir des preuves de contraventions », il a tout de même recommandé de modifier la *Loi sur les douanes* pour y intégrer des dispositions reprenant la politique de l'ASFC.

Projet de loi C-23 et zones de précontrôle à la frontière

Dans le contexte du projet de loi C-23, ***Loi sur le précontrôle (2016)***, le Commissariat s'est aussi penché sur la fouille des appareils électroniques, comme l'a indiqué le commissaire à plusieurs occasions.

En plus d'attirer l'attention sur la question au cours de sa comparution devant le Comité ETHI (mentionnée précédemment), le commissaire a réitéré ses préoccupations dans une lettre et une lettre de suivi adressées au Comité permanent de la sécurité publique et nationale de la Chambre des communes ainsi que dans le cadre d'une autre comparution devant ce comité et dans une lettre subséquente qui lui était adressée.

Dans ces mémoires, le commissaire a fait référence à des déclarations récentes du gouvernement américain affirmant que ses agents frontaliers pouvaient fouiller, à leur discrétion et sans aucun motif juridique, les appareils électroniques de tout étranger cherchant à entrer aux États-Unis. Ainsi, les agents pourraient exiger que ces étrangers fournissent le mot de passe de leur téléphone cellulaire ou de leurs comptes de médias sociaux.

En fin de compte, un agent américain pourrait contraindre un Canadien, même si ce dernier se trouve encore au Canada, à lui remettre son téléphone intelligent et à lui communiquer ses mots de passe à tout moment et sans motif, faute de quoi il pourrait lui refuser l'entrée aux États-Unis.

Au cours de chaque comparution et dans chaque mémoire, le commissaire a présenté, sous plusieurs formes, la recommandation du Commissariat visant à modifier la législation sur le précontrôle permettant ces fouilles (projet de loi C-23) de façon à mettre la fouille d'appareils électroniques à la frontière sur un pied d'égalité avec la fouille de personnes. Ainsi, elle ne pourrait être effectuée sans « motif raisonnable de soupçonner ».

Le Comité permanent de la sécurité publique et nationale de la Chambre des communes a fait la même recommandation, mais le projet de loi a été adopté sans modification importante en décembre 2017 et a par la suite reçu la sanction royale.

Même si le Commissariat a été incapable jusqu'à présent de convaincre les législateurs ou le gouvernement de modifier la loi dans le domaine, le gouvernement s'est engagé à lui présenter régulièrement des rapports sur le nombre de fouilles d'appareils numériques effectuées par l'ASFC.

De plus, le Commissariat mène actuellement plusieurs enquêtes liées à la sécurité nationale et à la surveillance exercée par le gouvernement. Nous constatons que les Canadiens sont de plus en plus préoccupés par la protection de la vie privée à la frontière et aux États-Unis.

Le Commissariat devrait présenter sous peu les conclusions de ses enquêtes sur la protection de la vie privée à la frontière. Entre-temps, il a mis à jour ses orientations sur le droit à la vie privée dans les aéroports et aux postes frontaliers afin de s'assurer que les Canadiens sachent à quoi s'attendre lorsqu'ils voyagent. Nous soulignons que les Canadiens voudront peut-être faire preuve de prudence et limiter le nombre d'appareils qu'ils prévoient apporter aux États-Unis, et vérifier et limiter les renseignements stockés sur les appareils qu'ils emportent avec eux.

RÉFORME DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS* ET ACTIVITÉS PARLEMENTAIRES

Depuis de nombreuses années, le Commissariat exhorte le gouvernement à moderniser la *Loi sur la protection des renseignements personnels*, la loi canadienne qui s'applique au secteur public fédéral.

Le Commissariat a indiqué clairement qu'une réforme de cette loi est absolument essentielle pour l'adapter aux changements technologiques et accroître la transparence. Les Canadiens conviennent qu'il est temps de moderniser la Loi, qui est demeurée pratiquement inchangée depuis son adoption en 1983.

Selon un sondage réalisé à la demande du Commissariat, dont les résultats ont été publiés au début de 2017, la majorité des Canadiens sont en faveur de modifications à la *Loi sur la protection des renseignements personnels*. En outre, les Canadiens souhaitent des rapports plus transparents avec le gouvernement et une reddition de comptes accrue.

Certains législateurs sont à l'écoute, mais le gouvernement tarde à prendre des mesures. Le Commissariat s'est réjoui lorsque le Comité ETHI a annoncé en mars 2016 qu'il étudierait la *Loi sur la protection des renseignements personnels*. Au terme de son étude, le Comité a produit un rapport final allant dans le sens de presque toutes les recommandations formulées par le Commissariat.

En avril 2017, dans sa réponse au rapport, le gouvernement a réitéré l'engagement, pris par la ministre de la Justice devant le Comité ETHI en 2016, d'examiner la *Loi sur la protection des renseignements personnels* pour la moderniser. Le gouvernement a affirmé que l'examen devrait « concrétiser les droits et les attentes des Canadiens en matière de protection des renseignements personnels, favoriser la confiance de la population et faciliter la bonne gouvernance pour notre démocratie du 21e siècle ».

Le Commissariat attend avec impatience l'examen par le gouvernement et demeure résolu à collaborer avec lui pour moderniser cette loi importante.

Activités parlementaires

En plus de formuler des avis au Parlement et de lui présenter des mémoires concernant les questions du consentement et du contrôle, le Commissariat a continué de surveiller et de commenter systématiquement d'autres nouveautés en matière de législation susceptibles d'avoir une incidence sur la vie privée des Canadiens.

Projet de loi C-58, *Loi modifiant la Loi sur l'accès à l'information et la Loi sur la protection des renseignements personnels*

En attendant que le gouvernement examine la *Loi sur la protection des renseignements personnels*, le commissaire a comparu devant le Parlement pour discuter de l'examen par le gouvernement de la *Loi sur l'accès à l'information*, qui a des répercussions sur la *Loi sur la protection des renseignements personnels*.

La Cour suprême a longtemps considéré la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels* comme un « code homogène » de droits en matière d'information. Les deux lois fonctionnent de pair et atteignent un juste équilibre entre la protection de la vie privée et l'accès à l'information. Dans des observations antérieures concernant la *Loi sur l'accès à l'information*, le Commissariat avait insisté sur l'importance de maintenir cet équilibre.

Le projet de loi C-58 n'a pas modifié les concepts clés d'exception relative à l'intérêt public ni la définition de « renseignements personnels ». Le Commissariat estime que c'est une bonne chose. Toutefois, le projet de loi confère à la commissaire à l'information le pouvoir d'ordonner la communication des documents du gouvernement, notamment ceux qui pourraient renfermer des renseignements personnels de Canadiens.

Au cours de sa comparution devant le Comité ETHI en octobre 2017, le commissaire a affirmé craindre que le projet de loi, en conférant à la commissaire à l'information le pouvoir de rendre des ordonnances, privilégie l'accès aux renseignements personnels plutôt que leur protection. Or, de toute évidence, ce pouvoir perturberait considérablement l'équilibre entre l'accès et la protection atteint dans la législation actuelle. Il irait à l'encontre de l'observation de la Cour suprême du Canada selon laquelle le droit à la vie privée l'emporte sur le droit d'accès à l'information.

Pendant sa comparution devant le Comité, le commissaire a recommandé plusieurs modifications au projet de loi. Entre autres, il a recommandé que le Commissariat soit consulté dans tous les cas où des renseignements personnels risquent vraiment d'être communiqués sans le consentement des intéressés.

Le projet de loi a été soumis au Sénat en décembre 2017 et renvoyé pour examen au Comité sénatorial permanent des affaires juridiques et constitutionnelles en juin 2018. Le Commissariat s'attend à recevoir une invitation à comparaître dans le cadre de l'étude.

Examen législatif de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* (LRPCFAT)

En février 2018, le commissaire a comparu devant le Comité permanent des finances de la Chambre des communes dans le cadre de l'examen législatif de la LRPCFAT. Le commissaire a réitéré les préoccupations soulevées par le Commissariat dans le passé. Il a aussi fait remarquer au Comité que cette loi permet de recueillir une grande quantité de renseignements sur les opérations financières de Canadiens respectueux de la loi dans le but de mettre au jour les menaces à la sécurité nationale ou les incidents de blanchiment d'argent.

Les renseignements en question sont recueillis par le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE). En vertu de la LRPCFAT, le Commissariat a le mandat de procéder, tous les deux ans, à l'examen des mesures prises par CANAFE en vue de protéger les renseignements qu'il reçoit ou recueille. Tous nos examens ont révélé des problèmes concernant la réception et la conservation de rapports par CANAFE non conformes aux seuils de déclaration prévus par la loi. Nous avons recommandé des améliorations et CANAFE a toujours répondu qu'il continuerait à mettre en œuvre des mesures de contrôle initial afin de réduire la quantité de renseignements personnels inutiles qu'il reçoit.

Par ailleurs, nous avons jugé que CANAFE a en général une approche efficace en matière de sécurité, entre autres des mesures de contrôle pour protéger les renseignements personnels. Notre dernière vérification a toutefois révélé des problèmes de gouvernance entre CANAFE et Services partagés Canada, qui conserve les données de CANAFE sur ses serveurs. CANAFE s'est engagé à les régler.

Le commissaire a formulé plusieurs recommandations au cours de sa comparution devant le Comité. Il a notamment recommandé de modifier la loi pour permettre au Commissariat de formuler des avis sur la proportionnalité dans le cadre de ses examens réguliers de la LRPCFAT. Dans son plus récent rapport annuel, CANAFE a déclaré avoir reçu presque 25 millions de dossiers en 2016-2017. Cependant, au cours de ce même exercice, il y a eu seulement 2 015 communications aux autorités chargées de l'application de la loi en vue d'éventuelles enquêtes.

Signalons que la durée de conservation des dossiers n'ayant fait l'objet d'aucune communication est de dix ans. Même si l'on admet que la communication de données relatives aux opérations financières concernant des citoyens respectueux de la loi peut mener à la découverte de menaces de blanchiment d'argent ou de financement d'activités terroristes, ces données ne devraient plus être conservées une fois que ces renseignements sont analysés et qu'ils permettent de conclure qu'une personne ne pose aucune menace.

Concernant les modifications qui pourraient être apportées aux lois et aux règlements, le commissaire a également recommandé que le ministère des Finances Canada soit tenu par la loi de consulter le Commissariat avant de déposer des projets de loi et de règlement ayant des répercussions sur la protection de la vie privée. Le gouvernement a recommandé de modifier la LRPCFAT pour que l'examen que nous effectuons actuellement tous les deux ans ait désormais lieu tous les quatre ans. Nous avons exprimé notre accord avec cette recommandation. Cependant, nous avons recommandé que les examens aient lieu au moins un an avant la date prévue de l'examen quinquennal devant être effectué par le Parlement.

Le Commissariat a exprimé ces points de vue dans son mémoire présenté dans le cadre des consultations sur la LRPCFAT menées par Finances Canada.

ENQUÊTES EN VERTU DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

Survol

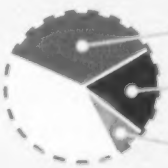
En 2017-2018, le Commissariat a accepté 1 254 plaintes déposées en vertu de la *Loi sur la protection des renseignements personnels*, soit une baisse de 8 % par rapport à l'exercice précédent. Par ailleurs, il a fermé 1 208 plaintes, soit 12 % de plus qu'en 2016-2017.

Le délai de traitement moyen par règlement rapide en 2017-2018 a été de plus de quatre mois, soit une augmentation de 7 % par rapport à l'exercice précédent. Le règlement des plaintes au moyen d'une enquête ordinaire a pris en moyenne presque 11 mois, soit un mois de plus que la norme des derniers exercices.

Malgré les efforts soutenus déployés pour traiter les plaintes par règlement rapide – plus d'un tiers des plaintes en vertu de la *Loi sur la protection des renseignements personnels* ont été réglées par ce moyen au cours des trois derniers exercices –, le délai de traitement moyen des plaintes a augmenté d'un mois au cours de l'exercice écoulé.

Les plaintes en chiffres

Institutions visées par le plus grand nombre de plaintes acceptées



Service correctionnel du Canada (35 %)

Gendarmerie royale du Canada (19 %)

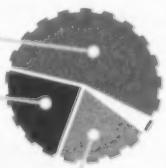
Défense nationale (7 %)

Types de plaintes les plus courantes

Délais (56 %)

Accès (24 %)

Protection des renseignements personnels (21 %)



Plusieurs éléments ont contribué à accroître le délai de traitement moyen, notamment la décision de se concentrer sur le règlement de plusieurs plaintes non résolues dans le système depuis un certain temps.

Surmonter les difficultés qui retardent le règlement des plaintes

Nous nous efforçons de terminer les enquêtes et de fermer les dossiers de plainte dans un délai de 12 mois, mais nous devons souvent composer avec des situations indépendantes de notre volonté.

Les plaintes reçues en vertu de la *Loi sur la protection des renseignements personnels* au cours des cinq dernières années sont beaucoup plus complexes en raison de l'utilisation toujours croissante des nouvelles technologies par les institutions fédérales. De plus, dans bien des cas, ces institutions peinent à répondre rapidement et complètement aux demandes d'information du Commissariat, si bien que les enquêtes sont plus longues et sollicitent davantage de ressources. D'après nous, il s'agit d'un symptôme du manque de ressources du bureau d'accès à l'information et de protection des renseignements personnels de certaines institutions.

Nous avons tout de même la responsabilité de gérer la situation de notre mieux et de continuer à chercher de nouveaux moyens de tirer le maximum de nos ressources d'enquête limitées. Nous avons entrepris depuis 2010 plusieurs initiatives pour aborder les questions ayant la plus grande incidence sur la vie privée et nous poursuivons ces efforts.

Par exemple, nous avons mis au point en 2017-2018 une nouvelle version du formulaire de plainte en ligne qui explique aux plaignants ce que le Commissariat peut et ne peut pas faire. À notre avis, le fait d'indiquer clairement notre rôle et notre mandat aux Canadiens nous aidera à leur offrir de meilleurs services. Nous avons l'intention de lancer le nouveau formulaire en 2018-2019. Cet outil devrait améliorer le processus de réception et d'enregistrement des plaintes. Nous avons également décidé de rédiger des rapports finaux plus courts dans les cas où le règlement rapide n'a pas été fructueux.

En utilisant un cadre de gestion des risques, nous avons créé un bassin de dossiers non attribués à faible risque. Ainsi, nous avons allégé la charge de travail de nos enquêteurs pour la ramener à un niveau gérable et pouvons consacrer davantage d'efforts aux enquêtes portant sur des enjeux à risque élevé d'atteinte à la vie privée des Canadiens.

Nous avons également embauché des ressources temporaires pour nous aider à fermer certains dossiers anciens qui présentent des défis particuliers, notamment des cas difficiles de relations de travail ou des dossiers faisant intervenir des institutions toujours lentes et peu coopératives dans leurs échanges avec le Commissariat. Dans l'ensemble, ces initiatives et d'autres mesures nous ont permis de réduire de près du tiers le nombre de plaintes ouvertes depuis plus d'un an, ce qui a ramené leur nombre total à 299 à la fin de l'exercice 2017-2018.

Enquêtes clés

Comme le montrent les exemples présentés ci-après, les enquêtes en vertu de la *Loi sur la protection des renseignements personnels* fermées au cours de l'exercice écoulé portaient sur une large gamme d'enjeux – collecte, utilisation et communication inappropriées de renseignements personnels, questions d'accès aux renseignements personnels détenus par des institutions fédérales, etc. Ces exemples nous aident aussi à comprendre comment la technologie a ajouté à la complexité des enquêtes sur les plaintes.

Le SCC efface encore une fois des enregistrements vidéo alors qu'une demande d'accès est à l'étude

Les conclusions de cette enquête ont suscité d'importantes préoccupations au Commissariat,

car l'institution fédérale en cause avait refusé de communiquer à une personne ses renseignements personnels tout comme elle l'avait fait plusieurs années auparavant.

Le plaignant, détenu dans un établissement fédéral, avait déposé auprès du Commissariat en 2011 une série de plaintes alléguant que le Service correctionnel du Canada (SCC) avait refusé de lui donner accès à ses renseignements personnels. Plus précisément, le SCC aurait refusé de lui transmettre des enregistrements vidéo qui, selon lui, montraient des agents correctionnels en train de l'agresser et de le harceler. D'après notre enquête, le SCC avait contrevenu à la *Loi sur la protection des renseignements personnels* en ne faisant aucun effort pour récupérer les enregistrements vidéo demandés par le plaignant pendant leur courte période de conservation. Le SCC avait tout simplement laissé le système vidéo écraser les enregistrements en question.

À l'époque, nous avions recommandé au SCC de mettre en place des mesures pour conserver et rendre accessibles les enregistrements qui sont gardés uniquement pour de courtes périodes (comme les enregistrements vidéo, qui sont écrasés après 4,5 jours) lorsque quelqu'un demande à y avoir accès.

En 2016, la même personne a communiqué avec le Commissariat pour indiquer que le SCC refusait encore une fois de lui donner accès à des enregistrements vidéo. Le SCC a indiqué refuser l'accès à certains enregistrements demandés pour des raisons de sécurité, comme le lui permet la Loi. En examinant ces vidéos, nous avons conclu que l'exception avait été appliquée de manière appropriée.

Cependant, en ce qui concerne d'autres enregistrements, nous avons jugé que le SCC n'avait pris aucune mesure pour récupérer les vidéos demandées par le plaignant avant leur écrasement. Or, le plaignant avait présenté sa demande dans un délai permettant de les récupérer. Nous avons conclu qu'il s'agissait d'une infraction grave à la *Loi sur la protection des renseignements personnels* et que la plainte concernant le refus d'accès aux renseignements était fondée.

Nous étions consternés de constater que, malgré nos conclusions antérieures selon lesquelles le SCC n'avait pas respecté la Loi ni appliqué nos recommandations visant à régler ce problème, l'organisme n'avait pris aucune mesure pour se conformer à la Loi. Nous avons réitéré notre recommandation et le SCC l'a acceptée. Dans sa réponse, l'organisme a déclaré qu'il rappellerait à ses employés leur obligation de s'assurer que les vidéos sont conservées et que toute demande d'accès s'y rapportant est traitée immédiatement. Le SCC fera rapport au Commissariat dans les six mois sur les mesures prises pour élaborer des processus efficaces afin de se conformer à la loi.

Consultez le rapport de conclusions d'enquête portant sur un refus d'accès au sein du SCC.

Utilisation d'un capteur IMSI à l'Établissement de Warkworth : le SCC responsable de l'interception de messages textes par un entrepreneur

Nous avons fait enquête sur plusieurs plaintes alléguant que le SCC utilisait un simulateur de site cellulaire pour capter et enregistrer sans autorisation des conversations par téléphone cellulaire et des messages textes à l'Établissement de Warkworth, en Ontario.

Les plaintes faisaient suite à un courriel envoyé au personnel par le directeur de l'établissement, qui mentionnait avoir autorisé le recours à un simulateur de site cellulaire (ou capteur IMSI) pour détecter l'utilisation de téléphones cellulaires par les détenus. Ces derniers n'ont pas droit aux téléphones cellulaires. Dans son courriel, le directeur a également indiqué qu'en plus de recueillir des renseignements sur l'emplacement et l'utilisation des téléphones cellulaires, le simulateur de site cellulaire enregistrait toutes les conversations vocales et tous les messages textes. Cependant, la dernière partie du message s'est par la suite révélée inexacte.

En vertu de la Loi, les seuls renseignements personnels que peuvent recueillir les institutions fédérales sont ceux qui ont un lien direct avec leurs programmes ou leurs activités.

Selon le SCC, les responsables soupçonnaient qu'une série d'incidents de sécurité dans l'établissement avaient impliqué l'utilisation de téléphones cellulaires par les détenus. Afin de régler ce problème, le SCC a retenu les services d'un entrepreneur pour utiliser un simulateur de site cellulaire afin de détecter la présence et l'utilisation de téléphones cellulaires à l'établissement. D'après le SCC, contrairement à l'information communiquée par le directeur dans son courriel, l'entrepreneur était autorisé à recueillir uniquement les métadonnées des téléphones cellulaires et non à enregistrer les conversations ou les messages textes. Toutefois, l'appareil a capté six messages textes.

Nous avons confirmé que les métadonnées de nombreux téléphones cellulaires utilisés dans l'établissement ont été recueillies. Puisqu'elles peuvent révéler l'identité et l'emplacement de l'utilisateur d'un téléphone cellulaire, les métadonnées constituent des renseignements personnels concernant un individu identifiable selon la définition de cette expression figurant dans la Loi. Les messages textes sont aussi des renseignements personnels.

En vertu de la Loi, les seuls renseignements personnels que peuvent recueillir les institutions fédérales sont ceux qui ont un lien direct avec leurs programmes ou leurs activités. Compte tenu du risque d'atteinte à la sécurité découlant de l'utilisation non autorisée de téléphones cellulaires à l'établissement, nous avons conclu que la collecte des métadonnées des téléphones cellulaires était conforme aux dispositions de la Loi régissant la collecte dans le cas en question.

En ce qui concerne les messages textes, nous n'avons trouvé aucun élément prouvant que le SCC avait demandé à l'entrepreneur de capter le contenu des communications des téléphones cellulaires. Toutefois, ces communications ont été captées dans le cadre d'une activité menée au nom du SCC. Puisque l'organisme est responsable des agissements de l'entrepreneur, il a contrevenu aux dispositions de la Loi régissant la collecte. Nous avons donc conclu que cet élément de la plainte était fondé.

Au cours de l'enquête, le SCC nous a informés qu'il n'avait pas l'intention d'utiliser des simulateurs de site cellulaire à l'avenir.

Consultez le rapport de conclusions d'enquête portant sur l'utilisation d'un capteur IMSI à l'Établissement de Warkworth.

Communication de dossiers médicaux par le MDN dans le cadre d'enquêtes sur des cas de mort subite

En vertu de l'alinéa 8(2)*e)* de la *Loi sur la protection des renseignements personnels*, une institution fédérale peut communiquer les renseignements personnels d'une personne sans son consentement à un organisme d'enquête qui en fait la demande par écrit en vue de faire respecter une loi ou pour la tenue d'enquêtes licites.

Dans le dossier en question, les plaignants alléguaient que la Direction de l'accès à l'information et de la protection des renseignements personnels du ministère de la Défense nationale (MDN) permettait généralement au Service national des enquêtes des Forces canadiennes (SNEFC) d'avoir accès au dossier médical des membres décédés des Forces canadiennes pour les enquêtes sur les cas de mort subite (suicides) sans prendre dûment en compte la nécessité de ces dossiers.

À titre d'exemple, les plaignants nous ont fourni une copie d'une demande présentée par le SNEFC à la Direction de l'accès à l'information et de la protection des renseignements personnels du MDN. Le SNEFC réclamait tous les documents se rapportant à la santé mentale du membre des Forces canadiennes ainsi que ses antécédents médicaux personnels et familiaux.

Selon la demande, les renseignements [traduction] « aideraient à déterminer si l'état d'esprit du membre

décédé des Forces canadiennes de même que tout problème de santé ou la prise de médicaments auraient pu affecter son état mental avant sa mort ».

Pour appuyer leur position, les plaignants nous ont invités à consulter la politique du SNEFC intitulée « Suicide et tentative de suicide » en vigueur à l'époque, qui indiquait :

> Les enquêtes sur les suicides ou les tentatives de suicide devraient déterminer que les blessures de la victime étaient, en fait, auto-infligées. […] Les détails administratifs (tentatives précédentes, causes possibles, état civil, dépendance d'alcool ou toxicomanie, etc.) ne doivent pas être activement recherchés […].

Les plaignants s'inquiétaient du fait que le SNEFC semblait être à la recherche de « détails administratifs » dans ses enquêtes et que le MDN lui communiquait plus de renseignements que nécessaire pour les besoins de ses enquêtes en lui acheminant des dossiers médicaux complets.

Pour sa part, le MDN a soutenu qu'il ne lui incombait pas de déterminer si le SNEFC agissait conformément à ses politiques internes et que, de toute manière, une enquête menée par la Commission d'examen des plaintes concernant la police militaire en 2015 avait conclu que les politiques du SNEFC relatives aux enquêtes portant sur les cas de suicide étaient trop contraignantes. Comme l'avait recommandé la Commission, la section de la politique affirmant qu'il n'était pas nécessaire de rechercher les détails administratifs a été supprimée.

Dans notre enquête, nous avons examiné les politiques du MDN et le traitement des demandes de renseignements médicaux présentées par le SNEFC à la Direction de l'accès à l'information et de la protection des renseignements personnels du MDN en vertu de l'alinéa 8(2)*e*) dans le cadre des enquêtes sur les cas de mort subite, notamment les suicides, sur une période de plusieurs années.

Nous avons conclu que la plainte n'était pas fondée. Nous avons souligné qu'il incombe à l'organisation communiquant les renseignements personnels de déterminer si l'organisme d'enquête qui les demande satisfait aux exigences de l'alinéa 8(2)*e*). Elle doit aussi acquérir une preuve *prima facie* que le demandeur cherche à obtenir uniquement des renseignements personnels directement liés à son enquête. D'après les demandes et les documents connexes que nous avons pu examiner au cours de l'enquête, nous sommes convaincus que le MDN s'acquitte effectivement de ses obligations à cet égard.

Nous avons tout de même constaté qu'une directive du Secrétariat du Conseil du Trésor (SCT) exige que l'article de la loi fédérale ou provinciale en vertu duquel l'activité d'enquête est entreprise soit énoncé dans une demande présentée en vertu de l'alinéa 8(2) *e*). Malgré cette exigence, les demandes présentées par le SNEFC que nous avons examinées indiquaient simplement comme motif la *Loi sur la défense nationale* ou une enquête sur un cas de mort subite.

Nous avons jugé que les communications étaient autorisées en vertu de la Loi, mais que le MDN avait omis dans certains cas de conserver une copie des demandes de communication à des organismes d'enquête fédéraux. La Loi et son règlement d'application exigent que les institutions conservent pendant au moins deux ans une copie de chaque demande reçue et tiennent un registre des renseignements communiqués.

Nous avons recommandé au MDN de mettre à jour ses politiques et ses procédures pour confirmer que le pouvoir en vertu duquel agit l'organisme d'enquête est indiqué dans les demandes présentées en vertu de l'alinéa 8(2)*e*) et que tous les documents se rapportant à ces demandes sont conservés comme l'exige la Loi.

Dans sa réponse, le MDN a accepté d'appliquer nos recommandations et de faire rapport au Commissariat dans les six mois.

Consultez le rapport de conclusions d'enquête portant sur le MDN.

Transports Canada exige l'inscription de renseignements personnels sur les drones

Nous avons fait enquête sur quatre plaintes alléguant que Transports Canada obligeait les propriétaires d'aéronefs sans pilote – souvent appelés « drones », « modèles réduits d'aéronefs » ou « véhicules aériens non habités » – à communiquer leurs renseignements personnels sans consentement.

Un arrêté d'urgence émis par Transports Canada en juin 2017 était au cœur du problème. Cet arrêté établissait plusieurs règles s'appliquant aux utilisateurs dits récréatifs des aéronefs sans pilote. L'arrêté indiquait notamment qu'« il est interdit au propriétaire d'un modèle réduit d'aéronef de l'utiliser, ou de permettre à une autre personne de l'utiliser, à moins que les nom, adresse et numéro de téléphone du propriétaire ne soient clairement visibles sur l'aéronef ».

Les plaignants ont souligné que tous les autres modes de transport sous réglementation fédérale et provinciale au Canada utilisent des numéros d'immatriculation pour identifier les véhicules, au lieu d'obliger les utilisateurs à mettre en évidence leurs coordonnées. Ils ont fait valoir que l'affichage des renseignements personnels sur les modèles réduits d'aéronefs exposait l'utilisateur à un risque de harcèlement ou de vol d'identité en cas de perte de l'appareil.

Transports Canada a indiqué que, selon les rapports sur les incidents impliquant les aéronefs sans pilote – qui ont augmenté de 200 % depuis 2014 –, les utilisateurs récréatifs de ces appareils, qui ont souvent une expérience limitée comme opérateurs, présentent des risques pour la sécurité aérienne ainsi que pour les personnes et les biens au sol. Le Ministère a indiqué avoir émis l'arrêté d'urgence en tant que mesure proactive pour réduire ces risques en attendant un règlement officiel.

Signalons que le nom, l'adresse et le numéro de téléphone d'une personne sont considérés comme des renseignements personnels et qu'ils ne peuvent pas être communiqués sans le consentement de l'intéressé. Cependant, les dispositions de la Loi régissant la communication ne s'appliquent qu'aux renseignements personnels relevant d'une institution fédérale. Dans le dossier en question, puisque l'arrêté exigeant l'inscription des renseignements sur les aéronefs sans pilote ne donne pas vraiment lieu à la collecte des renseignements personnels par Transports Canada, les dispositions de la Loi régissant la communication ne s'appliquent pas. Nous avons donc conclu que les plaintes n'étaient pas fondées.

L'arrêté indiquait notamment qu'« il est interdit au propriétaire d'un modèle réduit d'aéronef de l'utiliser, ou de permettre à une autre personne de l'utiliser, à moins que les nom, adresse et numéro de téléphone du propriétaire ne soient clairement visibles sur l'aéronef ».

Nous reconnaissons que tous les organismes de réglementation se heurtent à des défis liés aux aéronefs sans pilote, notamment en ce qui concerne la manière d'identifier facilement les opérateurs en cas de problème. En outre, contrairement à l'opérateur d'autres types de véhicules qui doit porter une pièce d'identité pendant le vol, l'opérateur d'un aéronef sans pilote ne se trouve pas physiquement au même endroit que son appareil. Nous en sommes conscients. Transports Canada a émis l'arrêté d'urgence en attendant l'approbation d'un règlement révisé qui devrait être publié dans la Partie II de la *Gazette du Canada* en 2018. Le Ministère a donné au Commissariat l'assurance que le nouveau règlement prendra en compte ses préoccupations en matière de protection de la vie privée. Même si nous n'avions aucune recommandation à formuler dans le contexte

de cette enquête, nous avons l'intention de surveiller l'élaboration du règlement final.

Consultez le rapport de conclusions d'enquête portant sur Transports Canada.

Statistique Canada : Des préoccupations légitimes, mais aucun risque accru pour les données de recensement

Un plaignant a déposé auprès du Commissariat une plainte alléguant que Statistique Canada avait communiqué de manière inappropriée des renseignements personnels confidentiels des Canadiens (recueillis pendant le recensement de 2016 et les recensements antérieurs) au moment du transfert à Services partagés Canada (SPC) de la gestion de son infrastructure de technologie de l'information.

De plus, selon le plaignant, il y a un risque de communication non autorisée à d'autres institutions fédérales puisque les données de Statistique Canada sont conservées dans des centres de données partagés avec ces ministères et organismes. Le plaignant déplorait que les employés de SPC ayant accès aux données de Statistique Canada ne soient pas supervisés par Statistique Canada. Il a demandé si ces employés avaient prêté serment de confidentialité en vertu de la *Loi sur la statistique* et si SPC collaborerait aux vérifications de la sécurité des données menées par Statistique Canada dans le but de détecter et d'atténuer tout risque d'atteinte à la sécurité.

En premier lieu, nous avons conclu que Statistique Canada n'avait pas communiqué les renseignements personnels des Canadiens de manière inappropriée.

Statistique Canada est tenu par la *Loi sur Services partagés Canada* d'utiliser les services d'infrastructure de TI offerts par SPC. En vertu de cette loi, les renseignements recueillis par les institutions fédérales peuvent être conservés dans ses systèmes de TI, mais ils ne relèvent pas de SPC et ne lui appartiennent pas. Dans le cas en question, les données demeurent donc la propriété de Statistique Canada et continuent de relever de l'organisme.

En ce qui concerne le risque de communication de données à d'autres ministères ou organismes, nous avons constaté que les données de Statistique Canada sont conservées dans un centre de données qui lui appartenait avant d'être cédé à SPC. De plus, ce centre se trouve dans une zone isolée d'un centre de données de SPC.

Par ailleurs, même si la propriété des centres de données a été transférée à SPC, l'infrastructure du recensement est physiquement séparée de celle des TI où sont stockées les données des autres ministères. En outre, des mesures de sécurité techniques et opérationnelles ont été mises en place pour réduire davantage le risque de communication non autorisée. Qui plus est, tous les employés de SPC qui ont accès à l'infrastructure du recensement, notamment d'anciens employés de Statistique Canada, sont officiellement réputés être des employés en vertu de la *Loi sur la statistique*. De ce fait, ils sont assujettis aux mêmes dispositions sur la sécurité que les employés de Statistique Canada.

Dans le cadre de notre enquête, nous avons aussi examiné les mesures prises par Statistique Canada pour s'assurer que les renseignements personnels des dizaines de millions de Canadiens recueillis au cours du recensement et transférés dans l'infrastructure de TI de SPC sont bien protégés. Nous avons consulté plusieurs documents fournis par Statistique Canada expliquant en détail son entente avec SPC et les contrôles mis en place pour protéger les données de recensement hébergées dans l'infrastructure de TI de SPC.

Signalons que le Commissariat avait déjà formulé plusieurs recommandations à Statistique Canada en réponse à l'Évaluation des facteurs relatifs à la vie privée que l'organisme lui avait présentée avant le recensement de 2016. À l'époque, nous lui avions recommandé de modifier cette évaluation de manière

à y indiquer les systèmes techniques relevant de SPC et à ajouter les évaluations des risques d'atteinte à la vie privée menées par SPC portant sur l'infrastructure technique relevant de ce ministère.

À la lumière de notre enquête, nous sommes convaincus que Statistique Canada a pris des mesures appropriées pour protéger les données détenues par SPC et réduire les risques associés au transfert de la gestion de son infrastructure de TI à ce ministère.

En conclusion, le plaignant a soulevé des préoccupations légitimes concernant les risques éventuels liés au transfert de la gestion de l'infrastructure informatique de Statistique Canada à SPC, mais nous avons conclu que la plainte n'était pas fondée. En effet, les renseignements personnels figurant dans les dossiers du recensement continuent d'appartenir à Statistique Canada et de relever de cet organisme. En fait, ces dossiers n'ont pas été communiqués à SPC. De plus, nous n'avons trouvé aucun élément prouvant un manquement de la part de Statistique Canada ou de SPC en ce qui concerne la protection adéquate des données contre toute communication non autorisée.

Consultez le rapport de conclusions d'enquête portant sur Statistique Canada.

Postes Canada : Communications non autorisées attribuables au système de réacheminement du courrier

La Société canadienne des postes (SCP) offre, moyennant des frais, un service de réacheminement du courrier qui permet à une personne de faire livrer son courrier à une autre adresse pendant une période pouvant atteindre un an. Il est possible d'acheter ce service sur le site Web de la SCP ou à un bureau de poste. Dans les deux cas, il faut présenter une preuve d'identité.

Les clients ont plusieurs moyens de confirmer leur identité. Entre autres, ils peuvent le faire en ligne en cliquant sur un lien qui mène à un service assuré par Equifax, agence d'évaluation du crédit. Le client doit répondre à une série de questions sur ses antécédents de crédit et d'autres renseignements personnels qui lui sont propres. S'il répond correctement à l'ensemble des questions, son identité est confirmée et il peut demander le réacheminement de son courrier.

Le réacheminement ne commence que trois jours ouvrables après la date d'achat du service. Selon la SCP, cette période constitue une mesure de sécurité. Pendant ces trois jours, la SCP envoie un avis de confirmation du réacheminement du courrier à l'ancienne adresse avant la date de début du service. Cet avis demande au destinataire de communiquer immédiatement avec la SCP s'il n'a pas acheté le service.

Dans le cas en question, une personne affirmant être le plaignant a utilisé le service en ligne pour faire réacheminer le courrier de ce dernier. Le lendemain du début du service, le plaignant a reçu un avis de confirmation du réacheminement du courrier en son nom. Il a immédiatement communiqué avec la SCP, qui a cessé de réacheminer son courrier.

Selon la SCP, l'envoi de l'avis de confirmation a été retardé en raison d'un problème technique, si bien que le plaignant ne l'a pas reçu avant le début du réacheminement de son courrier.

D'après notre enquête, un tiers avait pu se faire passer pour le plaignant en répondant correctement à toutes les questions posées par le système de vérification d'Equifax.

La SCP utilise l'avis de confirmation du réacheminement du courrier, une approche fondée sur le consentement implicite (« opt out »), pour s'assurer de la validité d'une demande de service. Cela signifie que la personne doit prendre des mesures si elle ne désire pas recevoir le service. Nous soulignons que le processus peut échouer si l'avis est perdu, n'est pas lu, ou, est retardé, comme dans le cas en question. D'après nous, la SCP doit élaborer et adopter une approche plus fiable pour régler ce problème.

Nous avons conclu que la plainte était fondée, puisque la SCP avait omis de prendre toutes les mesures

raisonnables pour s'assurer que les renseignements utilisés pour réacheminer le courrier du plaignant étaient exacts.

Au cours de notre enquête, la SCP a fait passer de trois à cinq jours la période prévue entre l'achat du service de réacheminement du courrier et le début du service. Ce changement aurait peut-être évité le réacheminement non autorisé du courrier du plaignant dans le cas en question, mais il n'aurait pas réglé le problème dans les cas où l'avis est remis plus de cinq jours après l'achat du service ou lorsque le destinataire perd l'avis ou ne le lit pas. Nous avons recommandé à la SCP d'envisager une approche plus fiable qui règle les problèmes soulevés pendant notre enquête et elle a accepté de le faire. Par conséquent, nous estimons que cette plainte est conditionnellement résolue.

Consultez le rapport de conclusions d'enquête portant sur Postes Canada.

Santé Canada : Collecte de renseignements détaillés sur la santé pour les demandes de remboursement des médicaments

Une plainte a été déposée au nom d'une vingtaine de médecins, selon lesquels Santé Canada les obligeait à recueillir plus de renseignements personnels que nécessaire afin de traiter les demandes de remboursement des médicaments pour les membres des Premières Nations et les Inuits dans le cadre du Programme des services de santé non assurés.

Plus précisément, la plainte portait sur le formulaire que les médecins doivent remplir pour le remboursement des médicaments figurant dans l'une des catégories de la Liste des médicaments, soit celle des « médicaments à usage restreint ». Le programme couvre les médicaments de cette catégorie uniquement si le patient remplit certains critères.

Les médecins concernés nous ont dit que Santé Canada exige dans de nombreux cas des renseignements diagnostiques exacts dans les formulaires des médicaments à usage restreint quand, selon eux, des renseignements généraux seraient suffisants pour démontrer que le patient remplit les critères. Par exemple, dans le formulaire de remboursement d'un médicament pour l'arthrite, on demande aux médecins de préciser le nombre d'articulations enflées.

D'après les médecins, comme les critères cliniques associés au médicament en question précisent qu'il vise à traiter les patients ayant une arthrite rhumatoïde active grave et au moins cinq articulations enflées, il devrait être suffisant d'indiquer que le patient se situe dans la plage exigée au lieu de préciser le nombre exact d'articulations enflées. Les médecins nous ont aussi cité des exemples de formulaires pour d'autres médicaments dans lesquels on leur demandait de donner des renseignements précis plutôt que d'indiquer la plage énoncée dans les critères cliniques.

Santé Canada a expliqué que les questions des formulaires reposent sur les critères cliniques établis par des comités de spécialistes chargés d'examiner les médicaments. Pour ce qui est du médicament contre l'arthrite, le nombre d'articulations enflées est demandé au début de la prise du médicament et au renouvellement de la prescription, généralement après un an. Selon les critères établis, si l'état du patient ne s'améliore pas de plus de 20 %, le médecin devrait changer la médication tant pour la sécurité du patient que pour des raisons de rentabilité. Santé Canada affirme ne pas pouvoir utiliser une plage de nombres d'articulations enflées pour effectuer ce calcul; il doit connaître le nombre exact.

À la lumière de l'information reçue de Santé Canada, nous avons conclu que les renseignements personnels demandés dans les formulaires de demande de remboursement pour les médicaments à usage restreint sont nécessaires. Ils servent directement à l'administration du Programme des services de santé non assurés et leur collecte est donc autorisée en vertu de la *Loi sur la protection des renseignements personnels*. Le Commissariat a conclu que cette plainte était non fondée.

Par ailleurs, les médecins nous ont affirmé que certains patients avaient exprimé des préoccupations quant à la façon dont Santé Canada conserve, utilise et communique leurs renseignements personnels, dont ceux ayant trait à leur santé mentale. Ces préoccupations dépassent la portée de notre enquête, mais elles montrent que les personnes accordent de l'importance à l'exercice d'un contrôle sur leurs renseignements personnels.

Nous avons encouragé le Ministère à communiquer avec les bénéficiaires du programme pour leur expliquer les pratiques de traitement des renseignements dans le cadre du programme. Nous avons déjà porté cette question à l'attention de Santé Canada. En faisant preuve d'une plus grande transparence, Santé Canada peut permettre aux bénéficiaires du programme d'exercer un contrôle sur leurs renseignements personnels.

Consultez le rapport de conclusions d'enquête portant sur Santé Canada.

Atteintes à la vie privée

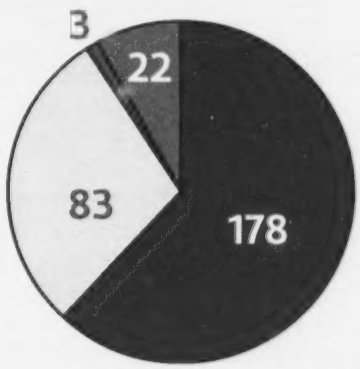
Les institutions fédérales sont tenues d'aviser le Commissariat et le Secrétariat du Conseil du Trésor de toute atteinte « substantielle » à la vie privée – c'est-à-dire si l'atteinte porte sur des renseignements personnels sensibles et qu'il serait raisonnable de penser qu'elle pourrait causer un dommage ou un préjudice grave à la personne concernée, ou si l'atteinte touche un grand nombre de personnes.

Il revient néanmoins aux institutions fédérales elles-mêmes de décider si une atteinte à la sécurité des données est substantielle et si elle doit même être déclarée. Aucune loi n'impose d'exigences à cet égard. Seule la politique du SCT s'applique. Nous avons recommandé de modifier la *Loi sur la protection des renseignements personnels* de façon à obliger les institutions fédérales à déclarer au Commissariat toute atteinte substantielle à la vie privée. Ainsi, nous serions plus à même de déterminer l'ampleur du problème dans l'ensemble du gouvernement et de formuler rapidement des avis et des recommandations pour gérer le risque.

En 2017-2018, nous avons reçu 286 déclarations d'atteinte à la vie privée au sein du secteur public. Il s'agit d'une forte hausse par rapport aux 147 atteintes déclarées en 2016-2017, mais près du quart de ces atteintes ont été déclarées par la même institution et dataient d'un an. Ces statistiques mettent en lumière la tendance à la baisse soutenue en ce qui concerne la déclaration des atteintes à la vie privée dans le secteur public.

D'après nous, ce n'est que la pointe de l'iceberg. En effet, nous sommes préoccupés par la réponse à une question inscrite au Feuilleton, qui a été présentée au Parlement concernant les atteintes à la vie privée au sein du gouvernement fédéral. Cette réponse révélait des milliers d'atteintes à la sécurité des renseignements des Canadiens. Sur ce nombre, au moins une demi-douzaine étaient de grande envergure et touchaient pas moins de 6 000 personnes, qui n'en avaient pas été avisées. Les institutions ne les avaient pas non plus déclarées au Commissariat.

TYPES D'ATTEINTES DÉCLARÉES



Cette information nous a incités à examiner la question de la déclaration des atteintes à la vie privée sous le régime de la *Loi sur la protection des renseignements personnels*. Notre examen, présenté en détail dans la prochaine section, a soulevé certaines préoccupations quant à savoir à quel point les institutions fédérales prennent au sérieux les renseignements personnels.

Examen des déclarations d'atteinte à la vie privée

Comme nous l'avons mentionné précédemment, le Commissariat a constaté une hausse constante du nombre d'atteintes à la sécurité des données dans le secteur public au cours des dernières années jusqu'en 2016-2017 – alors que le nombre de déclarations a chuté de plus de la moitié par rapport à l'exercice précédent. Comme l'indique le Rapport annuel 2016-2017, cette baisse nous a amenés à nous demander si les ministères appliquaient de façon uniforme les exigences en matière de déclaration des atteintes à la vie privée. Nous avons donc annoncé que nous effectuerions en 2017-2018 un suivi auprès des ministères afin de comprendre ce recul.

Examen des atteintes à la vie privée au sein du gouvernement fédéral

Que ce soit pour présenter une déclaration de revenus ou faire une demande d'assuranceemploi, de passeport ou de prêt d'études, les Canadiens n'ont souvent guère le choix de confier leurs renseignements personnels au gouvernement fédéral. Les institutions sont tenues de protéger ces renseignements en prenant des mesures de sécurité adéquates, mais notre examen des atteintes à la sécurité des données déclarées par le gouvernement a soulevé des préoccupations relativement aux mesures prises par les institutions pour prévenir et gérer ces atteintes.

Raison d'être de l'examen

Le Commissariat se sert des déclarations des atteintes en vertu de la *Loi sur la protection des renseignements personnels* qu'il reçoit des institutions fédérales pour cerner les menaces au droit à la vie privée et aider à déterminer les aspects où il faut formuler des avis, recommander des mesures correctives ou faire respecter la loi. C'est pourquoi nous avons amorcé l'examen des déclarations des atteintes à la sécurité des données au sein du gouvernement dans le but de faire un suivi concernant la baisse déconcertante du nombre de déclarations en 2016-2017 et d'autres enjeux liés à la déclaration des atteintes présentés dans notre rapport annuel précédent.

Soyons clairs : les enjeux n'ont pas changé depuis le dépôt de ce rapport. Le nombre d'institutions fédérales qui déclarent des atteintes au Commissariat demeure peu élevé et une très faible proportion de ces déclarations portent sur des cyberincidents[2]. De plus, nous continuons d'être informés d'incidents qui semblent être de graves atteintes à la vie privée par d'autres moyens, comme les médias – par exemple un reportage selon lequel des dossiers papier renfermant des renseignements personnels détaillés de centaines de Canadiens ont été perdus à la suite d'un vol de voiture.

Comment nous avons mené l'examen

Nous avons analysé les récentes déclarations d'atteintes en vertu de la *Loi sur la protection des renseignements personnels* et examiné les statistiques connexes du secteur public. Nous avons également demandé la collaboration d'une dizaine d'institutions fédérales détenant une grande quantité de renseignements personnels et examiné leurs procédures concernant les atteintes à la vie privée[3]. Le Commissariat n'a pas exercé ses pouvoirs d'enquête officiels, ce qui signifie que la participation des institutions était volontaire. À cet égard, nous tenons à les remercier pour leur temps, leurs efforts et leurs observations sincères.

2 Seulement deux cyberatteintes ont été déclarées en 2017-2018. Elles avaient eu lieu dans les systèmes de fournisseurs et non dans l'infrastructure du gouvernement. Comme nous l'avons indiqué dans notre Rapport annuel au Parlement 2016-2017, ce nombre négligeable de cyberatteintes est comparable à celui des années antérieures.

3 Réunions en personne avec les hauts fonctionnaires responsables de l'AIPRP, de la sécurité et des technologies de l'information de l'Agence des services frontaliers du Canada, de la Société canadienne des postes, de l'Agence du revenu du Canada, du ministère de la Défense nationale, d'Emploi et Développement social Canada, d'Affaires mondiales Canada, d'Immigration, Réfugiés et Citoyenneté Canada, de Services publics et Approvisionnement Canada, de Services partagés Canada et de Statistique Canada; mémoires du Service correctionnel du Canada et de la Gendarmerie royale du Canada.

Ce que nous avons appris

D'après les statistiques du gouvernement, il y a manifestement des milliers d'atteintes à la vie privée chaque année[4]. D'ailleurs, notre examen a clairement révélé que certaines atteintes substantielles ne sont pas déclarées et, qui plus est, d'autres encore passent fort probablement tout à fait inaperçues au sein de nombreuses institutions.

Nous avons demandé aux institutions si elles considéreraient la perte d'un passeport valide comme une atteinte substantielle (c'est-à-dire grave) à la vie privée. Les réponses variaient entre « oui », « non » et « tout dépend ».

Sur ce dernier point, bon nombre des institutions faisant l'objet de notre examen ont reconnu que leurs employés, surtout les travailleurs de première ligne, ne comprennent pas pleinement ce qui constitue un renseignement personnel ni les obligations leur incombant en vertu de la Loi. Il s'agit sans doute d'un des maillons faibles de la chaîne pour prévenir et gérer efficacement les atteintes à la vie privée.

La responsabilité de la protection des renseignements personnels pose également un problème. La déclaration des atteintes est obligatoire depuis quatre ans, mais nous avons constaté qu'il manque des éléments importants dans les procédures de détection et d'examen des atteintes de la plupart des institutions ayant pris part à notre examen. Certaines institutions ne se sont même pas dotées de procédures approuvées concernant les atteintes à la vie privée. Les institutions n'ont pas d'outils appropriés pour évaluer le risque de préjudice ou de tort causé aux personnes. Elles se concentrent plutôt sur le risque auquel est exposée leur propre organisation.

Notre examen a également confirmé que les mesures de sécurité des TI pour les nouveaux systèmes ne sont pas toujours à la hauteur, d'autant plus que ces systèmes servent toujours à traiter les renseignements personnels d'un grand nombre de personnes. Cette situation a très certainement été mise en évidence dans les conclusions de notre récente enquête sur une série d'incidents mettant en cause le système de paye Phénix. L'enquête a permis de déterminer que les atteintes à la vie privée découlaient d'une combinaison de facteurs – tests inadéquats, erreurs de codage et suivi et contrôle inefficaces du système[5].

Enfin, nous avons pu constater l'exaspération des institutions attribuable au fait que les directives et orientations concernant les atteintes à la vie privée sont appliquées de façon peu uniformes, parfois même ignorées ou considérées comme insuffisantes.

Observations du Commissariat et mesures connexes

Nous avons fait part de nos observations au SCT, qui est chargé de publier des directives et orientations à l'intention des institutions fédérales concernant l'administration de la *Loi sur la protection des renseignements personnels* ainsi que des règlements et politiques connexes. Plus précisément, nous avons communiqué au SCT les conclusions suivantes :

- Les lacunes par rapport à la déclaration des atteintes à la vie privée et les observations en ce qui concerne leur gestion en général font ressortir l'urgence d'apporter des améliorations et des éclaircissements au chapitre des orientations, de la formation et du soutien en ce qui a trait à la gestion des atteintes.
- Les mesures de sécurité sont probablement inefficaces à moins que les institutions ne prennent des mesures concrètes

4 Voir les réponses aux questions parlementaires écrites Q-427 et Q-1465.

5 Comme l'indique le rapport de conclusions, l'institution a par la suite accepté nos recommandations pour aider à résoudre les problèmes ayant contribué aux atteintes.

pour s'assurer que tous les employés comprennent bien ce qui constitue un renseignement personnel. Il faudrait en priorité sensibiliser les spécialistes des TI et de la sécurité à la protection de la vie privée, car le gouvernement reconnaît que « les cyberattaques sont de plus en plus envahissantes, sophistiquées et efficaces[6] ». De plus, la plupart des atteintes à la vie privée sont au départ des incidents de sécurité.

- Nous réclamons depuis bien des années une réforme de la *Loi sur la protection des renseignements personnels*, plus précisément l'ajout de dispositions particulières sur les mesures de sécurité et la déclaration obligatoire des atteintes. D'ailleurs, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI) appuie nos recommandations concernant la réforme législative.

Dans son quatrième rapport, le Comité ETHI recommande notamment de modifier la *Loi sur la protection des renseignements personnels* pour obliger d'obliger explicitement les institutions à protéger les renseignements personnels en prenant mesures physiques, organisationnelles et technologiques correspondant au niveau de sensibilité des données[7]. En réponse, le gouvernement a lancé un examen en vue de moderniser la Loi[8]. Nous attendons avec impatience l'adoption d'une loi modernisée protégeant le droit à la vie privée de tous les Canadiens.

Réponse du SCT

Le gouvernement du Canada prend au sérieux sa responsabilité fondamentale de protéger la confidentialité des renseignements personnels des Canadiens et Canadiennes. Le SCT est déterminé à veiller à ce que les renseignements personnels soient protégés, et il désire de poursuivre sa collaboration avec le CPVP pour renforcer la gestion des atteintes à la vie privée dans l'ensemble du gouvernement.

- Le SCT prépare un plan d'action pour l'automne 2018 qui énoncera des mesures précises assorties de délais précis visant à renforcer la gestion des atteintes à la vie privée dans l'ensemble du gouvernement.
- Dans le cadre de ce travail, le SCT examinera ses politiques, ses outils et sa formation pour tous les employés, ainsi que pour les spécialistes de la protection des renseignements personnels, de la sécurité et de la TI, afin de cerner les possibilités de renforcer l'orientation et les outils pour repérer, déclarer et gérer les atteintes à la vie privée. À titre d'exemple, le SCT travaillera avec l'École de la fonction publique du Canada pour passer en revue le « Cours de base sur l'accès à l'information et la protection des renseignements personnels » et le cours « Sensibilisation à la sécurité » afin de renforcer leur contenu touchant la protection des renseignements personnels, ainsi que le recensement et la déclaration des atteintes à la vie privée.
- Le SCT prendra des mesures pour sensibiliser les employés du gouvernement à ce qui constitue des renseignements personnels et à leur responsabilité en matière de déclaration des atteintes à la vie privée, la priorité étant accordée aux spécialistes de la TI et de la sécurité. À titre d'exemple, le SCT mettra au point des outils personnalisables de sensibilisation à la protection des renseignements personnels et préparera des présentations, des brochures et d'autres produits que les institutions du gouvernement du Canada peuvent utiliser

6 Budget de 2018 : Égalité + Croissance – Une classe moyenne forte, p. 230 (https://www.budget.gc.ca/2018/docs/plan/budget-2018-fr.pdf).

7 Rapport 4 – Protéger la vie privée des Canadiens : Examen de la Loi sur la protection des renseignements personnels, section 2.3 (http://www.noscommunes.ca/DocumentViewer/fr/42-1/ETHI/rapport-4/page-51).

8 Réponse du gouvernement au quatrième rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (http://www.noscommunes.ca/DocumentViewer/fr/42-1/ETHI/rapport-4/reponse-8512-421-135).

pour sensibiliser les employés à la protection des renseignements personnels et aux atteintes à la vie privée, notamment dans le contexte de la Semaine de la sensibilisation à la sécurité.

- Le SCT travaillera avec le ministère de la Justice Canada pour veiller à ce que les normes législatives en matière de sécurité des données et la déclaration obligatoire des atteintes à la vie privée soient prises en compte dans le cadre de l'examen de la *Loi sur la protection des renseignements personnels*.

Prochaines étapes

Au cours des prochains mois, le Commissariat lancera en collaboration avec le SCT son nouveau formulaire de rapport sur les atteintes en vertu de la *Loi sur la protection des renseignements personnels* pour les institutions du gouvernement du Canada. Le but est de faciliter la déclaration, d'aider les institutions à gérer les atteintes et de clarifier le processus.

En outre, le Commissariat donnera des conseils concernant la gestion des atteintes au sein du secteur public et en fera activement la promotion par les canaux de communication et de sensibilisation tant traditionnels que modernes et novateurs.

Plus important encore, toutefois, nous exhortons le gouvernement à mettre à profit les conclusions de cet examen pour combler les lacunes cernées, selon l'ordre de priorité, afin de protéger adéquatement les renseignements personnels des Canadiens.

AVIS AU GOUVERNEMENT

La principale responsabilité du Commissariat consiste à protéger le droit à la vie privée des Canadiens. Comme le commissaire l'a mentionné dans son message, nous avons récemment apporté des changements à notre structure organisationnelle afin de simplifier notre travail et d'adopter en matière de protection de la vie privée une approche plus proactive et percutante.

Cette nouvelle approche suppose que nous mettons davantage l'accent sur les pouvoirs donnés aux citoyens. Il s'agit aussi de travailler de façon proactive avec les organisations – dans la mesure où nos ressources limitées le permettent – pour mieux comprendre et atténuer les effets négatifs des programmes et des activités, y compris les technologies, sur la vie privée. En formulant des avis et en communiquant de l'information dès la conception des nouveaux programmes ou des nouvelles activités, nous devrions aider les Canadiens à profiter des avantages de l'innovation sans risque indu d'atteinte à la sécurité de leurs renseignements personnels.

Afin de mieux concentrer les efforts sur notre travail proactif auprès des institutions fédérales, nous avons créé dans le cadre de notre restructuration la Direction des services-conseils au gouvernement. Cette direction a pour mandat de formuler des avis et des recommandations concernant des programmes et initiatives en particulier. Elle examine également les évaluations des facteurs relatifs à la vie privée (EFVP) et les ententes d'échange de renseignements présentées au Commissariat par les ministères et organismes fédéraux. La direction mène aussi des activités de sensibilisation au sein du secteur fédéral afin de favoriser la conformité.

Consultations auprès des institutions fédérales

En vertu de la Politique sur la protection de la vie privée du SCT, les institutions fédérales doivent aviser le commissaire à la protection de la vie privée du Canada de toute initiative prévue ayant un lien avec la *Loi sur la protection des renseignements personnels* ou pouvant avoir une incidence sur la vie privée des Canadiens. Elles doivent l'aviser dès le

début du processus de planification pour permettre au commissaire d'examiner sérieusement l'initiative proposée et d'analyser toute question de protection de la vie privée avec les représentants du ministère concerné.

En vertu de la politique, les institutions fédérales doivent consulter le Commissariat. Par ailleurs, nous communiquons régulièrement avec elles de façon informelle afin de leur formuler des avis, des suggestions et des recommandations concernant des initiatives pouvant avoir une incidence sur le droit à la vie privée des Canadiens.

En 2017-2018, des ministères nous ont consultés sur toute une gamme d'initiatives donnant lieu à la collecte, à l'utilisation et à la communication de renseignements personnels des Canadiens. Plusieurs exemples sont cités dans le présent rapport.

Transports Canada et le Forum économique mondial : Identité numérique de voyageur digne de confiance

Transports Canada travaille avec le Forum économique mondial et le secteur privé à l'élaboration d'une identité numérique pour les voyageurs. Le Canada envisage de mettre à l'essai cette technologie au cours des prochaines années.

Selon Transports Canada, grâce à l'identité numérique de voyageur digne de confiance, les organismes gouvernementaux et les organisations du secteur privé de différents pays auraient accès, avec le consentement des intéressés, à leurs données biométriques et biographiques et à l'historique de leurs déplacements.

Grâce à ces renseignements, les organismes seraient en mesure de confirmer l'identité des voyageurs et d'évaluer le risque qu'ils présentent avant leur arrivée.

Parallèlement, ces identités numériques faciliteraient les déplacements internationaux en permettant aux voyageurs d'utiliser leur téléphone pour avoir accès aux points de contrôle pour les transports et à la frontière grâce à la technologie de reconnaissance biométrique.

D'après ses concepteurs, on pourrait adapter cette technologie pour l'utiliser dans plusieurs secteurs de l'économie, notamment ceux des soins de santé et des services bancaires. Au cours de nos consultations, nous avons formulé à leur intention des avis et des recommandations préliminaires concernant la gestion des risques d'atteinte à la vie privée, notamment l'importance de protéger les renseignements personnels liés à l'identité numérique de voyageur digne de confiance, de limiter la durée de conservation des renseignements et de restreindre les utilisations secondaires.

Nous étions heureux d'avoir été invités à donner notre avis compte tenu de l'ampleur et de la sensibilité des renseignements personnels qui seraient en cause. Nous prévoyons consulter régulièrement le Ministère à mesure que le projet pilote évoluera.

Programme d'examen des plaintes d'agression sexuelle des FAC et modèle de Philadelphie utilisé par la GRC aux fins de l'examen de ce type de plaintes

La Gendarmerie royale du Canada (GRC) et les Forces armées canadiennes (FAC) ont toutes deux consulté le Commissariat concernant leur plan d'action pour examiner les enquêtes antérieures sur les agressions sexuelles. Les deux organisations envisageaient d'adopter une variante du modèle dit de Philadelphie.

Cette approche consiste entre autres à confier à un organisme de surveillance l'examen des dossiers de plaintes pour agression sexuelle qui ont été jugés non fondés. Cet organisme serait composé d'intervenants et de professionnels externes ainsi que de représentants des services de police.

Compte tenu de la nature particulièrement sensible des renseignements personnels qui seraient communiqués à des tiers dans le cadre de ce processus, nous avons insisté sur le besoin criant d'évaluer pleinement les risques d'atteinte à la vie privée. Nous avons recommandé à la GRC et aux FAC de s'assurer de ne communiquer que les renseignements nécessaires à l'examen.

Nous avons également recommandé aux institutions de réfléchir à la façon d'informer les personnes touchées par les plaintes initiales de la communication éventuelle de leurs renseignements personnels à un organisme externe.

Après nous avoir consultés, les FAC nous ont fait parvenir une évaluation des facteurs relatifs à la vie privée (EFVP), dans laquelle elles s'engageaient à publier sur leur site Web un avis décrivant leur programme d'examen des plaintes d'agression sexuelle. Nous leur avons formulé certaines recommandations supplémentaires après avoir examiné leur EFVP, mais il était encourageant de constater que celle-ci reflétait bon nombre des recommandations que nous avions formulées quand les FAC nous avaient consultés. Mentionnons la mise en place de mesures visant à restreindre l'accès aux dossiers sensibles et l'obligation pour les membres de l'organisme de surveillance de signer une entente de confidentialité.

Pour sa part, la GRC a indiqué que son programme en était encore au stade exploratoire. Elle s'est engagée à collaborer avec le Commissariat s'il devait aller de l'avant.

Enquête nationale sur les femmes et les filles autochtones disparues et assassinées : Fin de l'élimination des anciens dossiers à la GRC

Par suite de l'émission d'un avis de préservation des documents dans le cadre de l'Enquête nationale sur les femmes et les filles autochtones disparues et assassinées, la GRC a temporairement cessé d'éliminer les dossiers de plusieurs systèmes de gestion des dossiers opérationnels. Les dossiers en question avaient atteint la fin de leur période de conservation et auraient normalement été supprimés, mais la GRC les a conservés afin de préserver des renseignements pouvant être importants dans l'enquête.

Compte tenu des risques liés à la conservation de renseignements pendant de longues périodes, nous avons recommandé à la GRC d'examiner les dossiers qui sont censés être supprimés et d'éliminer tout renseignement si elle peut confirmer qu'il n'est pas visé par l'ordonnance de préservation au lieu de cesser complètement d'éliminer les anciens dossiers.

Nous lui avons également recommandé de limiter l'accès aux renseignements conservés pour se conformer à l'ordonnance; de s'assurer que les renseignements ne sont pas utilisés à d'autres fins; et d'émettre un avis public pour indiquer que les dossiers en question seront conservés pendant une période prolongée.

Après nous avoir consultés, la GRC nous a appris que les responsables de l'enquête avaient précisé la portée de l'avis de préservation. Elle a repris le processus d'élimination des dossiers en conséquence, conformément aux périodes de conservation prescrites.

Utilisation de l'analyse des données : ARC, IRCC et ASFC

Au cours de l'exercice écoulé, nous avons consulté plusieurs institutions fédérales afin de discuter du recours à l'analyse des données et à l'intelligence artificielle pour l'exécution de certains programmes et de formuler des avis à ce sujet :

- le projet pilote d'analyse prédictive pour les visas de résident temporaire d'Immigration, Réfugiés et Citoyenneté Canada (IRCC), qui utilise l'analyse prédictive et la prise de décision automatisée dans le cadre des processus d'approbation des visas;
- l'utilisation par l'Agence des services frontaliers du Canada (ASFC) de l'analyse avancée dans le cadre de son Programme national de ciblage afin d'évaluer l'information sur les passagers pour tous les voyageurs aériens arrivant au Canada ainsi que son utilisation accrue prévue de l'analyse pour évaluer les risques liés aux personnes;

- l'utilisation croissante de l'analyse avancée par l'Agence du revenu du Canada (ARC) pour trier, catégoriser et coupler les renseignements sur les contribuables en fonction des indicateurs perçus de risque de fraude et de non-conformité.

Nous reconnaissons le potentiel de l'analyse avancée pour accroître l'efficience du gouvernement et appuyer de nouveaux modes de prestation des services aux Canadiens. En revanche, lorsque ces institutions nous ont consultés, nous avons constaté que ces technologies peuvent également encourager une augmentation de la collecte, du partage et du couplage des données.

Par conséquent, ces technologies peuvent également s'avérer envahissantes, intrusives et discriminatoires, selon la façon dont elles sont utilisées. Nous avons souligné que l'on devrait les adopter uniquement après un examen attentif des répercussions sur la vie privée. Il faudrait notamment évaluer la nécessité d'avoir recours à l'analyse en premier lieu et déterminer si le risque d'atteinte à la vie privée connexe est proportionnel aux résultats escomptés.

Il est essentiel de prendre en compte le risque d'atteinte à la vie privée dès maintenant, alors que l'application de l'analyse des données et de l'intelligence artificielle en est encore à ses débuts au sein du gouvernement. Il s'agit, entre autres, d'étudier des moyens de restreindre la collecte des renseignements personnels aux éléments essentiels pour le fonctionnement efficace de la technologie; d'assurer l'exactitude continue des renseignements stockés dans ces systèmes; et de garantir la transparence, la reddition de comptes et l'accès – particulièrement en ce qui concerne l'information sur la façon dont les algorithmes influent sur les décisions prises à l'égard des personnes.

Bureau du Conseil privé : Consultations en ligne auprès des jeunes

Le Bureau du Conseil privé a lancé un processus en ligne pour encourager les Canadiens âgés de 15 à 30 ans à faire part de leurs idées sur les thèmes et les priorités que les politiques gouvernementales devraient prendre en compte à leur avis. Les jeunes pouvaient exprimer leur opinion de façon anonyme. De plus, ils avaient la possibilité de participer à des forums en ligne ou de télécharger leurs propres rapports en s'inscrivant sur le site Web.

Les participants pouvaient également télécharger des vidéos sur le site Web des consultations au moyen de l'application tierce GoodTalk. On leur demandait de s'assurer au préalable d'avoir le consentement de toutes les personnes figurant dans leur vidéo, notamment les mineurs.

Le Bureau du Conseil privé a indiqué que toutes les vidéos proposées seraient examinées avant leur affichage sur le site, mais sans expliquer clairement comment il s'y prendrait pour confirmer que toutes les personnes y figurant avaient effectivement donné leur consentement. Nous avons suggéré que le Bureau du Conseil privé obtienne le consentement écrit de toutes les personnes figurant dans les vidéos dans le cas de futures initiatives comprenant l'affichage de contenu vidéo proposé par des utilisateurs. Cette exigence est particulièrement importante lorsqu'il s'agit de personnes mineures.

Statistique Canada : Utilisation accrue de sources de données administratives

Nous avons consulté Statistique Canada à plusieurs reprises au cours des dernières années pour discuter des répercussions de la collecte par cet organisme de données administratives sur la vie privée, par exemple les relevés de téléphone mobile, les rapports des agences d'évaluation du crédit et les factures d'électricité des individus. Nous avons de nouveau discuté avec des représentants de Statistique Canada à ce sujet pendant l'exercice écoulé, après que

plusieurs entreprises nous eurent fait part de leurs préoccupations relativement aux demandes de renseignements sur les clients émanant de l'organisme.

Statistique Canada affirme utiliser ce type de renseignements pour en apprendre davantage sur diverses tendances de la consommation, par exemple en matière de tourisme et de voyages. Ces données aident aussi à valider d'autres renseignements nécessaires, comme l'adresse des ménages et leur statut en matière d'habitation. D'après l'organisme, l'utilisation de dossiers administratifs existants coûte moins cher que les autres modes de collecte de renseignements tout en allégeant le fardeau des répondants.

Statistique Canada nous a informés qu'il supprime les identificateurs personnels et qu'il n'utilise les renseignements qu'à des fins de statistiques et de recherche. Toutefois, de nombreux Canadiens seraient étonnés d'apprendre que le gouvernement recueille leurs renseignements de cette façon et à cette fin.

Nous avons recommandé à l'organisme de déterminer s'il peut atteindre les mêmes objectifs en recueillant des renseignements qui ont été anonymisés avant de lui être communiqués. Nous lui avons également suggéré de limiter la collecte de données administratives aux éléments nécessaires aux fins prévues et d'évaluer en continu la nécessité et l'efficacité de ce travail. Afin d'assurer la transparence, nous recommandons à Statistique Canada d'indiquer à la population canadienne comment et pourquoi il intensifie la collecte de données provenant de sources administratives et d'autres sources non traditionnelles.

Élections Canada : Registre des futurs électeurs

Élections Canada et Immigration, Réfugiés et Citoyenneté Canada (IRCC) ont informé le Commissariat du transfert de nouvelles données sur la citoyenneté d'IRCC à Élections Canada en vertu du projet de loi C-33, *Loi modifiant la* Loi électorale du Canada *et d'autres lois en conséquence*.

Dans le projet de loi C-33, le gouvernement fédéral propose de créer un registre des futurs électeurs. Ainsi, les Canadiens âgés de 14 à 17 ans pourraient s'inscrire de leur propre gré afin que leurs renseignements soient automatiquement ajoutés au Registre national des électeurs lorsqu'ils atteindront l'âge de 18 ans. Les jeunes Canadiens n'ont pas besoin du consentement d'un parent ou d'un tuteur pour s'inscrire au registre. Toutefois, dans le cas des nouveaux citoyens canadiens de ce groupe d'âge, cette option figurerait dans la *Demande de citoyenneté canadienne – Enfants mineurs*, formulaire rempli par le répondant de la personne mineure. Si le parent ou le tuteur coche la case voulue, IRCC transmettra à Élections Canada le nom, l'adresse, la date de naissance, le sexe et l'identificateur unique de client du jeune citoyen.

Cela signifie que l'on pourrait inscrire au registre le nom des nouveaux Canadiens mineurs et que les institutions fédérales pourraient s'échanger leurs renseignements personnels à leur insu. Nous avons recommandé à IRCC d'examiner la question du consentement valable dans le cadre de l'évaluation des risques d'atteinte à la vie privée connexe.

Orientation sur les personnes politiquement exposées et les dirigeants des organisations internationales

Certaines personnes occupent un poste qui peut les rendre vulnérables à la corruption. Par exemple, une personne politiquement exposée ou le dirigeant d'une organisation internationale occupe un poste de premier plan lui permettant d'influer sur les décisions et d'exercer un contrôle sur les ressources

En vertu de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* du Canada, les institutions financières doivent déterminer si une personne est un étranger ou un national politiquement vulnérable ou encore le dirigeant d'une

organisation internationale ou un membre de sa famille ou une personne à laquelle elle est étroitement associée.

Des mesures accrues de diligence raisonnable, comme l'établissement de la source de fonds pour les comptes et certaines opérations financières, sont exigées pour tous les étrangers ou nationaux politiquement vulnérables et les dirigeants d'organisations internationales qui présentent un risque élevé de commettre une infraction de recyclage des produits de la criminalité ou une infraction de financement des activités terroristes.

En juin 2017, le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE) a publié une nouvelle directive à l'intention des institutions financières relativement à ces types de titulaires de compte. Nous avons constaté que la nouvelle directive omet de préciser si la diligence raisonnable accrue s'applique lorsqu'un national politiquement vulnérable ou le dirigeant d'une organisation internationale est considéré comme étant un client à faible risque. À notre avis, il s'ensuit un risque de collecte excessive de renseignements personnels auprès de personnes présentant un faible risque.

Nous avons recommandé à CANAFE de modifier sa directive pour préciser que, sauf lorsque la loi ou le règlement l'exige, les mesures de diligence raisonnable accrue ne s'appliquent pas aux nationaux politiquement exposés ni aux dirigeants d'organisations internationales à faible risque. Le Centre a accepté notre recommandation.

Dans sa réponse, CANAFE s'est engagé à modifier sa directive pour apporter cette précision et à publier une foire aux questions afin d'accroître la transparence des obligations en la matière à l'égard des personnes politiquement exposés et des dirigeants d'une organisation internationale.

Évaluations des facteurs relatifs à la vie privée (EFVP)

En vertu de la *Politique sur la protection de la vie privée* du SCT, les institutions fédérales doivent consulter le Commissariat dès le début de l'élaboration d'initiatives pouvant avoir une incidence sur la vie privée. Par ailleurs, la *Directive sur l'évaluation des facteurs relatifs à la vie privée* les oblige à bien évaluer les risques d'atteinte à la vie privée afin de les atténuer avant la mise en œuvre d'un programme en réalisant une EFVP.

Les institutions sont tenues de soumettre leurs EFVP à l'examen du Commissariat, qui peut recommander des mesures pour mieux gérer les risques d'atteinte à la vie privée. Nos recommandations et nos conseils ne sont pas contraignants, mais la plupart des institutions reconnaissent l'importance d'une approche proactive en matière de protection de la vie privée et travaillent en collaboration avec le Commissariat afin d'améliorer les mesures de protection dans le domaine.

ARC : Échange de renseignements avec les autorités fiscales étrangères

Depuis nombre d'années, l'Agence du revenu du Canada (ARC) et les autorités fiscales d'autres pays s'échangent des renseignements sur les contribuables en vertu de plusieurs conventions fiscales bilatérales. La *Norme commune de déclaration* est une nouvelle norme internationale concernant l'échange automatique de renseignements relatifs à des comptes financiers entre administrations fiscales. Elle vise à lutter contre l'évasion fiscale.

En vertu de la Norme, les institutions financières canadiennes déclarent à l'ARC les comptes détenus par des non-résidents du Canada ou par certaines entités contrôlées par des non-résidents du Canada. Par la suite, l'ARC envoie ces renseignements aux autorités fiscales du pays de résidence des personnes concernées, conformément à des accords officiels. Il en va de même pour les autorités fiscales étrangères, qui

envoient à l'ARC des renseignements sur les comptes détenus par des résidents du Canada.

Au cours de l'examen de l'EFVP, nous avons eu quelques préoccupations concernant la collecte excessive et l'utilisation éventuelles des renseignements personnels par l'ARC. De plus, nous avons reçu l'EFVP avant la réalisation de plusieurs évaluations de la menace et des risques. Par conséquent, nous n'avions aucun moyen de savoir si les risques associés au transfert de données de l'ARC aux autorités fiscales étrangères ont été cernés et gérés.

Nous étions également préoccupés par le fait que l'EFVP n'indiquait pas ce que le Canada avait fait ou prévoyait faire pour s'assurer que les administrations destinataires ont mis en place de mesures de sécurité adéquates afin de protéger les renseignements communiqués dans le cadre des ententes. Nous avons rencontré des représentants de l'ARC pour discuter de ces questions. Au moment de la rédaction du présent rapport, nous mettions la dernière main à des ententes en vue d'examiner la documentation pertinente, notamment les dossiers d'évaluation de la menace et des risques et de vérification de sécurité, les accords bilatéraux et les rapports d'évaluation de la confidentialité et de la protection des données propres à chaque administration.

ARC : Programme communautaire des bénévoles en matière d'impôt

Chaque année, des bénévoles remplissent environ 500 000 déclarations de revenus pour des personnes à faible revenu dans des comptoirs de préparation de déclarations organisés par des organismes communautaires ou d'autres groupes. L'ARC parraine ces comptoirs et inscrit les bénévoles qui remplissent les déclarations. La grande majorité des bénévoles souhaitent uniquement redonner à leur communauté, mais certaines atteintes à la sécurité des renseignements personnels recueillis ont été déclarées au Commissariat dans le passé.

L'ARC a présenté au Commissariat une EFVP sur son Programme communautaire des bénévoles en matière d'impôt. Toutefois, cette évaluation portait uniquement sur les risques d'atteinte aux renseignements personnels recueillis par l'ARC lorsque des bénévoles et des organismes communautaires s'inscrivent au programme.

L'EFVP ne comprenait aucune évaluation des risques d'atteinte à la vie privée liés au traitement des renseignements personnels par les bénévoles, notamment le risque d'utilisation inappropriée ou frauduleuse de ces renseignements. Entre autres, le Commissariat a recommandé à l'ARC d'élargir la portée de ses évaluations pour examiner tous les aspects du programme.

ASFC : Bornes d'inspection primaires

En mars 2017, l'ASFC a commencé à mettre en place des bornes d'inspection primaires et lancé l'application mobile connexe FrontièreCan – Déclaration électronique utilisée pour déterminer l'admissibilité des personnes ou des marchandises arrivant au Canada par voie aérienne. Après l'atterrissage au Canada, les voyageurs sont dirigés vers une borne où ils peuvent numériser leur passeport, se faire prendre en photo et répondre à l'écran à une série de questions des services des douanes et de l'immigration. L'application permet aux voyageurs d'utiliser leur appareil mobile pour répondre à l'avance aux questions de base de la déclaration. Elle leur envoie un code de réponse rapide (QR) pouvant être numérisé à une borne.

La borne vérifie les renseignements dans plusieurs bases de données de l'ASFC et imprime ensuite un reçu qui comprend la photo du voyageur et les résultats de l'évaluation. Le voyageur remet le reçu à un agent de l'ASFC, qui le vérifie et autorise la personne à aller prendre ses bagages ou la renvoie à l'examen secondaire pour répondre à des questions supplémentaires.

Dans le cadre de notre examen de l'EFVP, les analystes techniques du Commissariat ont effectué un examen technique de l'application mobile FrontièreCan – Déclaration électronique pour évaluer le risque de fuites de données sur le Web. L'examen a confirmé que les données recueillies par l'application ne sont pas transmises et que les données temporaires stockées localement sont protégées adéquatement.

En réponse aux recommandations formulées par le Commissariat, l'ASFC a accepté de mettre à jour l'EFVP pour y ajouter des renseignements supplémentaires indiquant de quelle façon et à quel moment les renseignements personnels peuvent être communiqués à d'autres ministères et partenaires dans l'application de la loi. Par ailleurs, d'après nous, l'Agence n'a pas justifié la conservation des photos des voyageurs après le traitement à la borne.

Nous continuons également d'encourager l'ASFC à indiquer clairement aux voyageurs que l'utilisation des bornes est facultative. Les voyageurs qui le préfèrent peuvent les contourner (et éviter ainsi de se faire photographier) en se présentant directement à un agent de l'ASFC pour le contrôle.

Santé Canada : Programme d'inscription pour la production de cannabis à des fins médicales

Dans le cadre du programme d'inscription pour la production de cannabis à des fins médicales, les Canadiens peuvent s'inscrire auprès de Santé Canada pour posséder et produire du cannabis à des fins médicales. Entre autres responsabilités, Santé Canada reçoit et traite les demandes, vérifie les documents médicaux et délivre les certificats d'inscription.

À la suite de l'examen de l'EFVP pour le programme, nous avons recommandé des mesures pour remédier à plusieurs risques d'atteinte à la vie privée. En particulier, nous avons conseillé au Ministère de conclure des ententes officielles d'échange d'information avec les divers partenaires avec lesquels il échange des renseignements du programme. Nous l'avons aussi encouragé à limiter la collecte de renseignements personnels à ceux qui sont nécessaires pour administrer le programme. Par exemple, nous avons remis en question la nécessité de recueillir des renseignements non liés aux drogues pour la vérification des antécédents judiciaires.

De plus, nous avons demandé à Santé Canada des précisions en ce qui concerne les mesures en place pour gérer tout risque lié à la possibilité de « réidentification » des individus à partir des données anonymisées du registre communiquées aux municipalités. Nous lui avons également demandé d'expliquer aux Canadiens l'incidence de la légalisation prévue de la consommation de cannabis à des fins récréatives sur le programme et ce qu'il advient des renseignements personnels des individus lorsqu'ils décident de quitter le programme.

Rapport du Commissariat sur les EFVP historiques : Échange transfrontalier de renseignements sur la migration

Dans le cadre des efforts continus déployés pour assurer la sécurité nationale et mondiale, le Canada et ses partenaires internationaux échangent de plus en plus de renseignements pour évaluer les voyageurs qui arrivent à leur frontière. Au cours des dernières années, le Commissariat a examiné de nombreuses EFVP portant sur l'échange de renseignements à des fins liées à l'immigration, à l'asile ou à la détermination des déplacements ou a été consulté à ce sujet.

Compte tenu du nombre d'ententes d'échange de renseignements en place et de leur diversité, nous avons décidé d'en examiner un échantillon ainsi que les EFVP connexes. Le but était de cerner tout problème systémique ou tout risque d'atteinte à la vie privée non maîtrisé et de mieux comprendre l'évolution de ce type d'échanges transfrontaliers de renseignements.

Nous avons examiné plusieurs EFVP et consultations concernant des ententes d'échange de renseignements lancées par IRCC, l'ASFC et Sécurité publique Canada entre 2003 et 2016. Nous avons ensuite évalué les ententes en fonction d'un ensemble de critères communs.

Nous nous attendons à ce que ces ententes précisent quels renseignements personnels doivent être communiqués, à quel moment et pour quelle raison. Nous nous attendons également à ce que ces ententes renferment des dispositions limitant l'utilisation secondaire et le transfert ultérieur des renseignements personnels et indiquant les mécanismes de protection des renseignements, leur durée de conservation et les personnes responsables de s'assurer que ces dispositions sont respectées.

À cet égard, signalons que le *Document d'orientation pour aider à préparer des Ententes d'échange de renseignements personnels* publié par le SCT prévoit également plusieurs dispositions qui doivent figurer dans les ententes. Nous avons été déçus de constater que les dispositions énoncées par le SCT figuraient rarement dans les ententes que nous examinions. En outre, malgré les efforts déployés pour définir clairement les pratiques d'échange de renseignements, les dispositions n'étaient généralement pas à la hauteur de nos attentes.

Toutes les ententes que nous avons examinées expliquaient pourquoi les renseignements personnels étaient communiqués, mais bon nombre d'entre elles mentionnaient également des objectifs généraux, ce qui pourrait ouvrir la voie à des interprétations trop généreuses des circonstances dans lesquelles l'échange de renseignements est nécessaire.

De plus, pour indiquer quels renseignements peuvent être communiqués, la plupart des ententes examinées faisaient appel à des formulations comme « peut inclure ». Ce libellé semble aller à l'encontre de l'esprit de notre recommandation voulant que les institutions énumèrent exactement les renseignements personnels pouvant être communiqués et qu'elles limitent la communication à ceux figurant sur la liste.

Rares étaient les ententes d'échange de renseignements qui mentionnaient quoi que ce soit concernant la limitation des utilisations secondaires des renseignements communiqués. Celles qui évoquaient cette notion le faisaient uniquement dans des termes vagues. Nous avons remarqué que la plupart des ententes renfermaient à tout le moins quelques dispositions sur la sécurité et la conservation des données conformément à notre recommandation voulant que les ententes d'échange de renseignements indiquent précisément comment les renseignements personnels sont traités. Parallèlement, nous avons constaté que les ententes s'appliquent souvent à perpétuité, c'est-à-dire qu'il n'y a aucune date de fin ni aucune indication précisant que les modalités ou la nécessité de l'échange de renseignements seront examinées après une période déterminée.

Fait peut-être le plus important, notre examen a révélé que les consultations auprès du Commissariat avaient généralement une incidence positive sur l'élaboration et la rédaction d'ententes d'échange de renseignements. Cet effet était particulièrement manifeste lorsque le Commissariat était intervenu dès le début du processus ou que la réalisation d'une EFVP coïncidait avec la rédaction d'une entente, au lieu que de la suivre.

Dans ce contexte, nous sommes préoccupés par le fait que les activités d'échange transfrontalier de renseignements de l'ASFC et d'IRCC n'ont pas toutes fait l'objet d'une EFVP. Aucune politique n'exige officiellement la réalisation d'une EFVP pour les activités d'échange de renseignements, mais ces activités donnent lieu à l'utilisation de renseignements personnels à des fins administratives et exigent donc un certain niveau d'évaluation des facteurs relatifs à la vie privée.

Nous espérons discuter davantage avec les institutions concernant leurs activités d'échange transfrontalier de renseignements pour nous assurer que ces ententes sont assujetties à des mesures robustes de protection de la vie privée.

Séances de mobilisation

En plus de mener des consultations sur des initiatives et des activités particulières et de travailler aux EFVP, le Commissariat communique également avec les représentants ministériels des programmes et de la protection des renseignements personnels de façon proactive pour leur donner une orientation générale concernant l'analyse des risques et la réalisation d'examens internes des pratiques de traitement des renseignements personnels.

En 2017-2018, ce type de mobilisation proactive a donné lieu à une série de séances de mobilisation des intervenants auxquelles participaient des employés responsables des programmes et de la protection des renseignements personnels au sein de divers ministères et organismes fédéraux. En plus des nombreuses améliorations possibles suggérées, nous avons trouvé encourageant que les participants soulignent à maintes reprises que les avis et les conseils formulés par le Commissariat sont précieux – et qu'ils souhaiteraient nous consulter plus tôt et plus souvent, dans un cadre plus informel, afin d'obtenir davantage d'information pour leurs analyses des risques d'atteinte à la vie privée. Nous sommes déterminés à agir de la façon la plus proactive possible pour formuler aux ministères et aux organismes des avis utiles en temps opportun.

Dossiers relatifs à la protection de la vie privée devant les tribunaux

Le Commissariat continue à suivre les causes devant les tribunaux pouvant avoir une incidence sur le droit à la vie privée des Canadiens et, s'il y a lieu, à intervenir dans ces dossiers.

DOSSIERS AUXQUELS LE COMMISSARIAT A PARTICIPÉ AU COURS DE L'EXERCICE ÉCOULÉ

Procureur général du Canada c. Larry Philip Fontaine et autres, 2017 CSC 47

En octobre 2017, confirmant une décision de la Cour d'appel de l'Ontario, la Cour suprême du Canada a statué que les survivants des pensionnats devraient exercer un contrôle sur le sort final des documents clés issus du Processus d'évaluation indépendant (PEI) en vertu de la Convention de règlement relative aux pensionnats indiens (CRRPI).

Le gouvernement du Canada soutenait que les documents issus du PEI, qui présentent des histoires personnelles de sévices racontées par des milliers de survivants, constituaient des documents fédéraux soumis à la *Loi sur la protection des renseignements personnels*, à la *Loi sur l'accès à l'information* et à la *Loi sur la Bibliothèque et les Archives du Canada*.

Devant la Cour suprême, tout comme devant la Cour d'appel de l'Ontario, le Commissariat a agi en tant qu'intervenant. Il a souligné l'importance de s'assurer que les survivants des pensionnats exercent un contrôle sur ces renseignements très personnels.

La Cour suprême du Canada a conclu qu'en vertu de la CRRPI, il revient aux survivants des pensionnats de décider si les documents présentant leurs histoires doivent être archivés ou détruits après une période de 15 ans.

Union of Canadian Correctional Officers – Syndicat des agents correctionnels du Canada – CSN (UCCO-SACC-CSN) c. Procureur général du Canada-A-463-16 (Cour d'appel fédérale) (décision en délibéré)

Nous attendons actuellement une audience devant la Cour d'appel fédérale, qui déterminera si une décision rendue par la Cour fédérale du Canada sur les vérifications obligatoires de solvabilité pour les agents correctionnels sera confirmée ou non.

Comme nous l'avons indiqué dans notre Rapport annuel 2016-2017, la Cour fédérale a conclu que l'utilisation des renseignements sur la solvabilité est autorisée en vertu de l'article 4 de la *Loi sur la protection des renseignements personnels*, car ces renseignements ont un lien direct avec le programme de filtrage de sécurité du SCT puisqu'ils peuvent aider à évaluer la vulnérabilité d'un agent à la corruption. De plus, la Cour fédérale a conclu que, contrairement aux arguments invoqués par le Commissariat, l'article 4 de la *Loi sur la protection des renseignements personnels* n'exige pas que la collecte des renseignements personnels soit nécessaire aux programmes ou aux activités d'une institution fédérale.

En qualité d'intervenant dans la procédure initiale et l'appel, le Commissariat fait valoir que, selon son interprétation de l'article pertinent de cette loi, les institutions fédérales doivent limiter les renseignements personnels qu'elles recueillent à ceux qui sont nécessaires à leurs programmes. Autrement dit, les institutions doivent montrer que la collecte des renseignements personnels est « nécessaire » aux programmes, et non simplement « utile ».

Sa Majesté la Reine c. Ryan Jarvis, CSC 37833 (décision en délibéré)

Nous attendons une décision dans ce dossier concernant un enseignant d'une école secondaire qui utilisait une caméra-stylo pour enregistrer des vidéos d'étudiantes, visant souvent leur poitrine. L'enseignant a d'abord été acquitté du chef d'accusation de voyeurisme, car le tribunal a conclu que la preuve n'était pas suffisante pour établir que les vidéos avaient été faites « dans un but sexuel ».

La Cour d'appel de l'Ontario a jugé que les vidéos avaient été faites dans un but sexuel, mais elle a confirmé l'acquittement au motif que celles-ci avaient été enregistrées dans des circonstances pour lesquelles il n'existait aucune attente raisonnable de protection de la vie privée – élément clé de l'infraction de voyeurisme. Selon le raisonnement d'une majorité de juges, les étudiants qui sont à l'école doivent s'attendre à être observés et éventuellement enregistrés.

Un juge avait présenté une opinion dissidente, soutenant que les étudiants, quand ils sont à l'école, ont une attente raisonnable de protection de la vie privée à l'égard de toute personne cherchant à porter atteinte à leur intégrité personnelle et sexuelle. Cette opinion a servi de fondement à un appel devant la Cour suprême du Canada, qui a été entendu en avril 2018.

Le Commissariat a été l'un des intervenants autorisés à présenter un mémoire officiel dans cet appel. Nous avons fait valoir que l'« attente raisonnable de protection de la vie privée » ne dépend pas uniquement du lieu. Même dans un cadre public ou semi-public, comme une école ou un bureau, les personnes devraient être en mesure de s'attendre à ce que l'on ne porte pas atteinte à certains aspects de leur vie privée. À notre avis, l'approche limitée et fondée sur le lieu qui a été adoptée par la majorité des juges de la Cour d'appel de l'Ontario minerait le droit à la vie privée des Canadiens dans diverses situations.

DOSSIERS QUE NOUS AVONS SUIVIS AVEC INTÉRÊT

En plus des dossiers où il a joué un rôle actif en tant qu'intervenant, le Commissariat a suivi avec intérêt plusieurs autres dossiers devant les tribunaux portant sur des questions de protection de la vie privée.

Entre autres, nous nous sommes intéressés à plusieurs affaires entendues par la Cour suprême du Canada :

- Dans *Douez c. Facebook* (2017 CSC 33), la Cour a rendu une décision sur l'applicabilité de la clause d'élection de for dans les contrats de consommation type lorsqu'il y a une incidence sur le droit à la vie privée. Elle a conclu qu'un tribunal en Colombie-Britannique peut examiner une plainte pour atteinte à la vie privée déposée par une personne dans cette province et que la plainte n'a pas à être déposée en Californie comme le prévoient les conditions d'utilisation de Facebook.
- Dans deux causes distinctes, soit *R. c. Marakah* (2017 CSC 59) et *R. c. Jones* (2017 CSC 60), la Cour a conclu que, selon les circonstances, les personnes peuvent s'attendre raisonnablement à ce que leurs messages textes demeurent confidentiels, même après leur envoi.

Google Inc. c. Equustek Solutions Inc. (2017 CSC 34) n'avait eu aucune incidence directe sur la vie privée, mais cette cause présentait un intérêt particulier du fait qu'elle portait sur des situations où il est possible d'ordonner au propriétaire d'un moteur de recherche de supprimer (déréférencer) des renseignements dans ses résultats de recherche.

La Cour a également examiné la « portée extraterritoriale des ordonnances des tribunaux ». Il s'agissait de déterminer si un tribunal canadien a compétence pour rendre une ordonnance visant une entreprise qui n'est pas physiquement présente au Canada afin de prévenir un préjudice sur Internet. Ces deux questions pourraient avoir une incidence sur la mesure dans laquelle nous pouvons exercer un contrôle sur nos renseignements personnels sur Internet. La section du présent rapport consacrée au consentement et au contrôle fait état de certaines répercussions sur le droit à la vie privée de l'arrêt *Equustek*, notamment en ce qui concerne la vie privée et la réputation.

Coopération avec des organisations canadiennes et internationales

Le Commissariat continue à travailler en collaboration avec les organisations analogues au Canada et dans d'autres pays afin de mieux régler les questions transfrontalières de protection de la vie privée et d'échanger des connaissances et des leçons tirées de l'expérience susceptibles d'améliorer les politiques et les normes de protection des renseignements personnels partout dans le monde. Nous formulons également des avis au gouvernement du Canada pour l'aider à définir ses positions concernant la vie privée dans les forums internationaux (p. ex. l'Organisation de coopération et de développement économiques et Coopération économique Asie-Pacifique).

CONFÉRENCE INTERNATIONALE DES COMMISSAIRES À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

Le commissaire Daniel Therrien a été élu pour un deuxième mandat de deux ans au sein du comité exécutif de la Conférence internationale des commissaires à la protection des données et de la vie privée au cours de sa 39e réunion annuelle en septembre 2017. Le comité exécutif surveille les activités de la conférence, qui constitue le premier forum mondial pour les organismes de protection des données et de la vie privée.

Faisant fond sur des travaux codirigés par le Commissariat l'an dernier consacrés à la collaboration dans l'application des lois, les participants ont adopté cette année une résolution en vue d'explorer les possibilités futures en matière de coopération transfrontière dans l'application des lois. Le Commissariat est l'un des auteurs de cette résolution.

De plus, les participants ont adopté une résolution sur la protection des données dans les véhicules automatisés et connectés. Le Commissariat avait voté en faveur de cette résolution. Il a également coparrainé une résolution sur l'amélioration de la collaboration entre les autorités de protection des données et celles de protection des consommateurs. Dans la foulée de l'adoption de cette résolution, il joue un rôle clé au sein du groupe de travail Citoyens et consommateurs numériques. Le Commissariat rédige actuellement son rapport, qui sera déposé au cours de la 40e conférence annuelle.

Conjointement avec le Commissariat à l'information et à la protection de la vie privée de l'Australie et avec la Federal Trade Commission des États-Unis, le Commissariat a reçu le grand prix du président pour l'innovation et le prix pour le règlement des différends, la conformité et l'application des lois au cours de la première cérémonie de remise des prix de la protection de la vie privée et des données de la Conférence internationale des commissaires à la protection des données et de la vie privée. C'est leur enquête conjointe sur le piratage du site Ashley Madison qui leur a valu ces prix.

AUTORITÉS DE PROTECTION DE LA VIE PRIVÉE DE LA ZONE ASIE-PACIFIQUE

En novembre 2017, nous avons organisé conjointement avec le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique le 48e Forum des autorités de protection de la vie privée de la zone Asie-Pacifique (APPA) à Vancouver. Sur le thème des partenariats pour la recherche, les discussions ont souligné combien les partenariats avec les intervenants de l'industrie, de la société civile et du milieu universitaire peuvent contribuer à alimenter et compléter les travaux de réglementation et d'application de la loi effectués par les autorités de protection des données. Par ailleurs, des présentations ont été données sur des travaux de recherche financés par le Programme des contributions du Commissariat.

GLOBAL PRIVACY ENFORCEMENT NETWORK (GPEN)

En collaboration avec le Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario, nous avons « ratissé » 27 applications en ligne fort utilisées dans les classes, depuis la maternelle jusqu'à la 12e année. Cet examen s'inscrivait dans le cadre du cinquième ratissage annuel du GPEN pour la protection de la vie privée. Le ratissage de mai 2017 portait sur les pratiques en matière de respect de la vie privée de services et d'outils éducatifs en ligne utilisés dans les classes. Les concepteurs de bon nombre des applications que nous avons examinées prennent des mesures importantes pour protéger la vie privée des enfants et des jeunes. Malheureusement, nous avons aussi relevé des cas où des applications et des sites Web éducatifs encourageaient les élèves à fournir de leur propre gré plus de renseignements personnels que nécessaire. En vue de la mise en commun des stratégies et des compétences en matière d'application de la loi, le GPEN a également organisé son premier atelier destiné aux spécialistes de l'application de la loi à Manchester, au Royaume-Uni. Le Commissariat a aussi codirigé cet atelier, qui a permis à divers organismes de réglementation de partout dans le monde de mettre en commun leur expérience.

LOI CANADIENNE ANTI-POURRIEL (LCAP)

Le Commissariat a été l'un des dix organismes qui ont participé au tout premier ratissage du Unsolicited Communications Enforcement Network (UCENet) dirigé par le Commissariat à l'information du Royaume-Uni et le Conseil de la radiodiffusion et des télécommunications canadiennes.

Ce ratissage portait sur le marketing d'affiliation, entente commerciale qui permet, par exemple, à un détaillant en ligne de verser une commission à un site Web externe dirigeant des consommateurs vers son site, souvent au moyen de messages textes ou de courriels non sollicités. Le ratissage du UCENet a permis de déceler plusieurs problèmes, par exemple la publicité trompeuse et l'absence du consentement des consommateurs. Plusieurs sites Web ont été ciblés pour un suivi par les organismes participants au ratissage.

Le Commissariat a joué un rôle dans deux examens de la LCAP cette année. Un examen interne mené en collaboration avec nos partenaires canadiens dans l'application de cette loi a produit des résultats généralement positifs. Il a toutefois suscité des revendications en faveur d'un partage accru de renseignements avec ces partenaires et d'activités de sensibilisation coordonnées.

Dans son rapport sur l'examen triennal obligatoire de la LCAP par le Parlement, le Comité permanent de l'industrie, des sciences et de la technologie de la Chambre des communes a proposé de donner davantage de souplesse au CRTC pour lui permettre de partager des renseignements avec ses partenaires chargés de l'application de la LCAP. Soulignons que nous avions recommandé cet assouplissement au chapitre de l'échange de renseignements entre les partenaires, notamment le Commissariat, au cours de la comparution du commissaire devant le Comité en octobre 2017.

COOPÉRATION FÉDÉRALE-PROVINCIALE-TERRITORIALE

Au cours de la réunion annuelle des commissaires à l'information et à la protection de la vie privée fédéraux, provinciaux et territoriaux (FPT), qui a eu lieu en octobre 2017 à Iqaluit, au Nunavut, nous nous sommes prononcés en faveur d'une résolution conjointe exhortant les gouvernements à s'assurer que leurs commissaires à l'information et à la protection de la vie privée ont le pouvoir d'ordonner aux institutions publiques de produire des documents pour lesquels elles invoquent des exceptions aux lois sur l'accès à l'information, notamment en raison du secret professionnel de l'avocat. Sans ce pouvoir, les commissaires n'ont aucun moyen de déterminer si ces exceptions sont légitimes.

Une autre collaboration FPT a porté sur la protection de la vie privée des jeunes. Conjointement avec nos partenaires, nous avons adressé au Conseil des ministres de l'Éducation une lettre demandant une meilleure intégration de la sensibilisation à la protection de la vie privée dans le programme visant l'acquisition de compétences numériques dans les écoles. Nous avons également collaboré avec nos collègues provinciaux et territoriaux à l'élaboration de plans de cours pour les enseignants.

En ce qui concerne l'application de la loi, les commissariats canadiens appliquant des lois essentiellement similaires (Alberta, Colombie-Britannique et nous-mêmes) ont continué à trouver des possibilités de collaboration et d'échange de renseignements par l'entremise du Forum national de collaboration sur l'application de la loi. De plus, en avril 2018, nous avons annoncé une enquête conjointe avec le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique pour déterminer si Facebook et AggregateIQ respectent la LPRPDE et la loi sur la protection des renseignements personnels de la Colombie-Britannique.

MOBILISATION PROACTIVE À L'ÉGARD DU SS7

Dans le cadre des efforts accrus déployés pour mener des initiatives plus proactives qui nous permettront de mieux comprendre les processus technologiques complexes et, par conséquent, d'aviser les organisations et de mieux protéger la vie privée des Canadiens, nous avons demandé de l'information sur le système de signalisation n° 7 (SS7). Il s'agit d'un ensemble de protocoles qui permet à différents réseaux de télécommunications de communiquer entre eux et d'échanger des données sur la connexion des appels, l'itinérance et la facturation.

Grâce à un reportage diffusé en novembre dernier par la CBC et la Société Radio Canada, nous avons pris connaissance d'une vulnérabilité en matière de sécurité se rapportant au SS7, qui était déjà connue au sein de l'industrie. Ce reportage montre que les pirates n'ont eu besoin que d'un numéro de téléphone pour suivre à la trace le téléphone cellulaire d'un député fédéral qui avait accepté de participer au reportage. D'après ce reportage et plusieurs autres, les pirates informatiques ciblent le SS7 pour obtenir les renseignements des abonnés, entendre leurs appels, leur voler de l'argent, mener des attaques par déni de service et géolocaliser leurs déplacements.

Pour mieux comprendre cet enjeu, son incidence sur la protection des renseignements personnels et les mesures d'atténuation à prendre ou prises au Canada et ailleurs dans le monde, nous avons communiqué avec les institutions fédérales qui se penchent déjà sur ce dossier. Nous avons également contacté l'Association canadienne des télécommunications sans fil, les compagnies canadiennes de télécommunications, un expert international et nos partenaires partout dans le monde.

Nous avons appris que le SS7 est un outil essentiel aux communications mondiales. Nous sommes conscients que des experts partout dans le monde, dont des entreprises de télécommunications et des organismes de sécurité gouvernementaux canadiens, sont au courant de cette vulnérabilité et qu'ils collaborent depuis un certain temps à atténuer les risques en découlant.

Certains pays européens, toutefois, semblent en avance sur le Canada pour ce qui est d'atténuer davantage cette vulnérabilité.

Dans le cadre de notre mobilisation proactive, nous avons exhorté les intervenants à prendre en considérations les recommandations qui suivent :

- prendre des mesures techniques et organisationnelles appropriées concernant la surveillance et le filtrage de la sécurité de la signalisation pour gérer les risques d'atteinte à la sécurité des réseaux et des services;
- se tenir au courant des pratiques exemplaires à l'échelle internationale visant à sécuriser l'interconnexion pour le SS7, notamment les pratiques exemplaires et les lignes directrices relatives à la sécurité de la GSMA (Global System for Mobile Communications Association), et adopter ces pratiques pour optimiser la protection;
- s'efforcer d'accroître la prise de conscience et la connaissance des problèmes du SS7 au sein de leurs équipes de sécurité et de prévention de la fraude.

Le Commissariat a jugé encourageant les engagements pris par les intervenants en réponse à notre invitation à appliquer ces recommandations; nous continuerons à suivre de près la situation pour assurer que les questions de protection de la vie privée demeurent une priorité au moment d'évaluer et d'atténuer les vulnérabilités du SS7. Cet enjeu illustre bien encore une fois l'importance d'être constamment à l'affût des menaces technologiques existantes et émergentes auxquelles sont confrontés les réseaux et les systèmes de communications.

Annexe 1 – Définitions

Types de plainte

Accès :
À la suite d'une demande officielle d'accès à l'information, l'institution ou l'organisation aurait refusé à une ou à plusieurs personnes l'accès aux renseignements personnels qu'elle détient à leur sujet.

Avis de prorogation :
En vertu de la *Loi sur la protection des renseignements personnels*, l'institution n'aurait pas donné une justification appropriée pour la prorogation, aurait fait la demande de prorogation après le délai initial de 30 jours ou aurait fixé l'échéance à plus de 60 jours après la date de réception de la demande.

Collecte :
L'institution ou l'organisation aurait recueilli des renseignements personnels non nécessaires ou les aurait recueillis par des moyens inéquitables ou illicites.

Consentement :
En vertu de la LPRPDE, une organisation a recueilli, utilisé ou communiqué des renseignements personnels sans le consentement valable de la personne en cause ou, pour le motif qu'elle fournit un bien ou un service, a exigé que la personne consente à une collecte, à une utilisation ou à une communication déraisonnable de renseignements personnels.

Conservation et retrait :
L'institution ou l'organisation n'aurait pas conservé des renseignements personnels selon le calendrier de conservation pertinent – les renseignements auraient été détruits trop rapidement ou conservés trop longtemps.

Correction ou annotation (accès) :
L'institution ou l'organisation n'aurait pas corrigé des renseignements personnels ou, en cas de désaccord avec les corrections demandées, n'aurait pas annoté le dossier pour en faire état.

Correction ou annotation (délais) :
En vertu de la *Loi sur la protection des renseignements personnels*, l'institution n'aurait pas corrigé les renseignements personnels ou n'aurait pas annoté le dossier en conséquence dans les 30 jours suivant la réception de la demande de correction.

Délais :
L'institution n'aurait pas répondu à une demande dans les délais prescrits par la *Loi sur la protection des renseignements personnels*.

Détermination des fins de la collecte des renseignements :
En vertu de la LPRPDE, une organisation n'a pas déterminé les fins de la collecte de renseignements personnels avant la collecte ou au moment de celle-ci.

Exactitude :
L'institution ou l'organisation n'aurait pas pris toutes les mesures raisonnables pour s'assurer que les renseignements personnels utilisés sont exacts, à jour et complets.

Frais :
L'institution ou l'organisation aurait exigé indûment des frais pour répondre à une demande d'accès à des renseignements personnels.

Langue :
En réponse à une demande présentée en vertu de la *Loi sur la protection des renseignements personnels*, l'institution ou l'organisation n'aurait pas fourni les renseignements personnels dans la langue officielle choisie par le demandeur.

Mesures de protection :
En vertu de la LPRPDE, une organisation n'a pas protégé par des mesures de protection appropriées les renseignements personnels qu'elle détient.

Possibilité de porter plainte :
En vertu de la LPRPDE, une organisation n'a pas mis en place des procédures ou des politiques permettant à une personne de porter plainte à l'égard du non-respect de la *Loi* ou elle a enfreint ses propres procédures et politiques.

Répertoire :
InfoSource (un répertoire du gouvernement fédéral qui décrit chaque institution et les banques de données – groupes de fichiers sur le même sujet – qu'elle possède) ne décrirait pas de façon adéquate le fonds de renseignements personnels d'une institution.

Responsabilité :
En vertu de la LPRPDE, une organisation ne s'est pas acquittée de ses responsabilités à l'égard des renseignements personnels en sa possession ou sous sa garde ou elle n'a pas désigné une personne responsable de s'assurer qu'elle se conforme à la *Loi*.

Transparence :
En vertu de la LPRPDE, une organisation n'a pas rendu facilement accessibles aux demandeurs des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels.

Utilisation et communication :
L'institution ou l'organisation aurait utilisé ou communiqué des renseignements personnels sans le consentement de la personne en cause ou les aurait utilisés ou communiqués de façon non conforme aux usages et aux communications prévus par la loi.

Décisions

Fondée :
L'institution ou l'organisation a enfreint une ou des dispositions d'une *Loi sur la protection des renseignements personnels*.

Fondée et résolue :
L'institution ou l'organisation a enfreint une disposition d'une *Loi sur la protection des renseignements personnels*, mais elle a par la suite pris des mesures correctives pour remédier à la situation à la satisfaction du Commissariat.

Fondée et conditionnellement résolue :
l'institution ou l'organisation a enfreint une disposition d'une *Loi sur la protection des renseignements personnels*. L'institution ou l'organisation s'est engagée à mettre en œuvre des mesures correctives satisfaisantes approuvées par le Commissariat.

Non fondée :
L'enquête n'a pas mis au jour des éléments de preuve suffisants pour conclure que l'institution ou l'organisation a enfreint une *Loi sur la protection des renseignements personnels*.

Résolue :

En vertu de la *Loi sur la protection des renseignements personnels*, l'enquête a révélé que la plainte découle essentiellement d'une mauvaise communication, d'un malentendu, etc., entre les parties, et/ou l'institution a accepté de prendre des mesures pour remédier à la situation à la satisfaction du Commissariat.

Réglée :

Le Commissariat a aidé à négocier en cours d'enquête une solution satisfaisante pour toutes les parties en cause et n'a publié aucune conclusion.

Abandonnée :

En vertu de la *Loi sur la protection des renseignements personnels* : L'enquête a pris fin avant que toutes les allégations ne soient pleinement examinées. Diverses raisons peuvent entraîner l'abandon d'un dossier, mais ce ne peut être à la demande du Commissariat. Par exemple, il est possible que le plaignant ne veuille pas poursuivre la démarche ou que l'on ne puisse trouver ses coordonnées afin qu'il fournisse des renseignements supplémentaires essentiels pour en arriver à une conclusion.

En vertu de la LPRPDE : L'enquête a pris fin sans qu'une conclusion n'ait été publiée. Le commissaire peut mettre fin à l'enquête à sa discrétion pour un motif prévu au paragraphe 12.2(1) de la LPRPDE.

Hors du champ d'application :

On a déterminé qu'aucune loi fédérale sur la protection des renseignements personnels ne s'applique à l'institution ou à l'organisation ou ne régit l'objet de la plainte. Par conséquent, le Commissariat ne produit aucun rapport.

Règlement rapide :

La situation a été réglée à la satisfaction du plaignant dès le début du processus d'enquête. Le Commissariat n'a publié aucune conclusion.

Refus d'enquêter :

En vertu de la LPRPDE, le commissaire a refusé d'amorcer l'examen d'une plainte, car il estime que le plaignant aurait d'abord dû épuiser les recours internes ou les procédures d'appel ou de règlement des griefs qui lui sont normalement offerts; que la plainte pourrait avantageusement être instruite selon d'autres procédures prévues par le droit fédéral ou provincial; ou que la plainte n'a pas été déposée dans un délai raisonnable après que son objet a pris naissance, comme le prévoit l'article 12(1) de la LPRPDE.

Retrait :

En vertu de la LPRPDE, le plaignant a retiré sa plainte volontairement ou ne pouvait plus être joint dans les faits. Le Commissariat ne publie aucun rapport.

Annexe 2 – Tableaux statistiques

STATISTIQUES RELATIVES À LA LPRPDE

Tableau 1

Plaintes en vertu de la LPRPDE acceptées*, par secteur de l'industrie

Secteur de l'industrie	Nombre	Proportion par rapport à l'ensemble des plaintes acceptées**
Aliments et boissons	2	1 %
Assurances	21	7 %
Divertissement	5	2 %
Éditeurs	3	1 %
Fabrication	4	1 %
Finances	70	24 %
Gouvernement	2	1 %
Hébergement	19	6 %
Internet	31	10 %
Organismes sans but lucratif	1	0 %
Personne	1	0 %
Santé	4	1 %
Services	43	14 %
Services professionnels	18	6 %
Télécommunications	40	13 %
Transports	17	6 %
Vente et commerce de détail	16	5 %
Total	**297**	**100 %**

* Plaintes en vertu de la LPRPDE acceptées en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 6.

** Les nombres ayant été arrondis, leur somme pourrait ne pas correspondre aux totaux indiqués.

Tableau 2

Plaintes en vertu de la LPRPDE acceptées*, par type de plainte

Type de plainte	Nombre	Proportion par rapport à l'ensemble des plaintes acceptées**
Accès	86	29 %
Consentement	70	24 %
Utilisation et communication	62	21 %
Mesures de protection	45	15 %
Collecte	15	5 %
Conservation	5	2 %
Exactitude	5	2 %
Transparence	3	1 %
Responsabilité	2	1 %
Correction ou annotation	2	1 %
Fins acceptables	1	0 %
Autre	1	0 %
Total	**297**	**100 %**

* Plaintes en vertu de la LPRPDE acceptées en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 6.

** Les nombres ayant été arrondis, leur somme pourrait ne pas correspondre aux totaux indiqués.

Tableau 3

Dossiers d'enquête* liés à la LPRPDE fermés, par secteur de l'industrie et décision

Secteur de l'industrie	Réglée rapidement	Décision (règlement rapide exclu)									Total partiel des décisions (règlement rapide exclu)	Total des règlements rapides et autres décisions
		Refusée	Abandonnée (article 12.2)	Hors du champ d'application	Retirée	Réglée	Non fondée	Fondée	Fondée et résolue	Fondée et conditionnellement résolue		
Aliments et boissons	1											1
Assurances	15		2		2	1	2		1		8	23
Divertissement	3								1		1	4
Éditeurs	1							1			1	2
Fabrication	5								1		1	6
Finances	48	2	13			2	4	1	3	1	26	74
Gouvernement	1			2							2	3
Hébergement	12		1			1			1		3	15
Internet	14		7	3	3	1	1	2		1	18	32
Organismes sans but lucratif	1									1	1	2
Personne				1							1	1
Santé	2		1						1		2	4
Services	33		1		1	1	1		2		6	39
Services professionnels	15		2		3		1	1	1		8	23
Télécommunications	28		6						5	1	12	40
Transports	15		4		1		3	2	1	2	13	28
Vente et commerce de détail	11					1			1		2	13
Non précisé									1		1	1
Total	**205**	**2**	**37**	**6**	**10**	**7**	**12**	**7**	**19**	**6**	**106**	**311**

* Enquêtes en vertu de la LPRPDE effectuées en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 8.

Tableau 4

Dossiers d'enquête* liés à la LPRPDE fermés, par type de plainte et décision

Type de plainte	Règlement rapide	Abandonnée (article 12.2)	Refusée	Hors du champ d'application	Retirée	Réglée	Non fondée	Fondée	Fondée et résolue	Fondée et conditionnellement résolue	Total
Accès	63	9	1	1	2	1	4	3	10	1	**95**
Utilisation et communication	43	12	1	1	2	1	2	2	4	1	**69**
Consentement	38	8		4	5	2	1	2	3	2	**65**
Mesures de protection	29	4				2			2	1	**38**
Collecte	8	2			1		3				**14**
Exactitude	11										**11**
Correction ou annotation	3	1					1				**5**
Transparence	4					1					**5**
Conservation	3										**3**
Responsabilité	2									1	**3**
Fins acceptables	1	1					1				**3**
Total	**205**	**37**	**2**	**6**	**10**	**7**	**12**	**7**	**19**	**6**	**311**

* Enquêtes en vertu de la LPRPDE effectuées en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 8.

Tableau 5

Enquêtes* en vertu de la LPRPDE – Délais de traitement moyens, par décision

Décision	Nombre	Délai de traitement moyen en mois
Résolue par règlement rapide	205	3,5
Abandonnée (article 12.2)	37	8,3
Fondée et résolue	19	19,0
Non fondée	12	18,0
Retirée	10	12,0
Fondée	7	13,2
Réglée	7	10,6
Fondée et conditionnellement résolue	6	19,6
Hors du champ d'application	6	6,6
Refusée	2	2,0
Nombre total de cas	**311**	
Moyenne générale pondérée		**6,1**

* Enquêtes en vertu de la LPRPDE effectuées en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 8.

Tableau 6

Enquêtes* en vertu de la LPRPDE – Délais de traitement moyens, par type de plainte et de règlement

	Règlement rapide		Autre règlement (sauf règlement rapide)		Toutes les enquêtes	
Type de plainte	Nombre de cas	Délai de traitement moyen en mois	Nombre de cas	Délai de traitement moyen en mois	Nombre de cas	Délai de traitement moyen en mois
Accès	63	2,8	32	13,1	95	6,3
Utilisation et communication	43	2,4	26	9,7	69	5,2
Consentement	38	2,6	27	12,6	65	6,8
Mesures de protection	29	2,7	9	11,8	38	4,8
Collecte	8	4,7	6	17,3	14	10,1
Exactitude	11	3,8			11	3,8
Transparence	4	2,5	1	13,3	5	4,7
Correction ou annotation	3	2,2	2	7,7	5	4,4
Fins acceptables	1	6,0	2	19,5	3	15,0
Responsabilité	2	1,4	1	39,0	3	13,9
Conservation	3	0,9			3	0,9
Total	**205**	**2,7**	**106**	**12,6**	**311**	**6,1**

* Enquêtes en vertu de la LPRPDE effectuées en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 8.

Tableau 7

Déclarations volontaires des atteintes en vertu de la LPRPDE, par secteur de l'industrie et type d'incident

Secteur	Type d'incident				Total des incidents par secteur	Pourcentage par rapport à l'ensemble des incidents*
	Communication accidentelle	Perte	Vol	Accès non autorisé		
Agriculture, foresterie, pêche et chasse				1	1	1 %
Assurances	5		1	1	7	6 %
Divertissement			1	1	2	2 %
Éditeurs				1	1	1 %
Extraction minière et extraction de pétrole et de gaz	1		3		4	3 %
Fabrication				3	3	3 %
Finances	12	2	3	10	27	23 %
Gouvernement	1	1		1	3	3 %
Hébergement	2		1	5	8	7 %
Internet				5	5	4 %
Organismes sans but lucratif	5		2	3	10	9 %
Santé	1		2	1	4	3 %
Services	2		2	7	11	9 %
Services professionnels				3	3	3 %
Télécommunications	2		2	3	7	6 %
Transports	1			3	4	3 %
Vente et commerce de détail	1			10	11	9 %
Non précisé	1	1	1	2	5	4 %
Total	**34**	**4**	**18**	**60**	**116**	**100 %**

* Les nombres ayant été arrondis, leur somme pourrait ne pas correspondre aux totaux indiqués.

TABLEAUX STATISTIQUES LIÉS À LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

Tableau 1

Décisions sur les plaintes* relatives à l'accès et à la protection des renseignements personnels en vertu de la LPRP, par institution

Intimé	Abandonnée	Hors du champ d'application	Non fondée	Résolue	Réglée	Fondée	Fondée et résolue	Résolue par règlement rapide	Total
Administration canadienne de la sécurité du transport aérien								1	1
Affaires autochtones et du Nord Canada								5	5
Affaires mondiales Canada								1	1
Agence canadienne d'inspection des aliments							1	5	6
Agence de la santé publique du Canada								1	1
Agence des services frontaliers du Canada	4		2		2		3	36	47
Agence du revenu du Canada	8		13	1		1		31	54
Agence Parcs Canada				1				2	3
Agriculture et Agroalimentaire Canada								1	1
Anciens Combattants Canada		2	4	1		2		10	19
Banque du Canada								1	1
Bibliothèque et Archives Canada								6	6
Bureau de l'enquêteur correctionnel								2	2
Bureau du Conseil privé			1			1	1	2	5
Centre d'analyse des opérations et déclarations financières du Canada			1					2	3
Centre de la sécurité des télécommunications Canada			1					3	4
Comité de surveillance des activités de renseignement de sécurité								1	1
Commissariat à l'information du Canada	1					2		1	4
Commissariat à l'intégrité du secteur public du Canada								1	1
Commissariat aux langues officielles							2		2
Commission canadienne des droits de la personne							1	2	3
Commission de l'immigration et du statut de réfugié du Canada	2		1					4	7
Commission de la fonction publique du Canada				1				6	7
Commission des libérations conditionnelles du Canada	1		1			1	1	8	12
Conseil de la radiodiffusion et des télécommunications canadiennes	1								1
Conseil national de recherches Canada					1			2	3

Intimé	Abandonnée	Hors du champ d'application	Non fondée	Résolue	Réglée	Fondée	Fondée et résolue	Résolue par règlement rapide	Total
Diversification de l'économie de l'Ouest Canada								1	1
École de la fonction publique du Canada					1			1	2
Élections Canada								1	1
Emploi et Développement social Canada	4		5		1	1	1	14	26
Environnement et Changement climatique Canada			1	4					5
Gendarmerie royale du Canada	6	1	4		3	10	3	48	75
Immigration, Réfugiés et Citoyenneté Canada	1		4		3			20	28
Innovation, Sciences et Développement économique Canada	2							1	3
Marine Atlantique S.C.C.								1	1
Ministère de la Défense nationale	4		5	1	4	1		19	34
Ministère de la Justice Canada			3		1		2	6	12
Musée canadien de l'histoire	1								1
Office national de l'énergie								1	1
Pêches et Océans Canada			1			1		1	3
Ressources naturelles Canada			1	1		1		2	5
Santé Canada			1					4	5
Secrétariat du Conseil du Trésor du Canada								1	1
Sécurité publique Canada			2					2	4
Service Canada			1					3	4
Service canadien d'appui aux tribunaux administratifs								1	1
Service canadien du renseignement de sécurité	1		9		1			20	31
Service correctionnel Canada	6		9	2	6	6	5	56	90
Services partagés Canada								3	3
Services publics et Approvisionnement Canada	1					2	1	8	12
Société canadienne d'hypothèques et de logement			1						1
Société canadienne des postes	4					1		15	20
Société Radio-Canada								1	1
Statistique Canada	1							9	10
Technologies du développement durable du Canada			1						1
Transports Canada	2		1	1			1	6	11
Tribunal canadien des droits de la personne	1								1
Tribunal des anciens combattants (révision et appel)								1	1
VIA Rail Canada								2	2
Total	**51**	**3**	**73**	**13**	**23**	**30**	**22**	**382**	**597**

* Plaintes en vertu de la LPRP fermées en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 26.

Tableau 2

Délais de traitement des plaintes en vertu de la LPRP – Règlement rapide, par type de plainte*

Type de plainte	Nombre	Délai de traitement moyen en mois
Accès	**221**	**3,54**
Accès	214	3,57
Correction ou annotation	7	2,83
Délais	**59**	**1,65**
Protection des renseignements personnels	**161**	**5,79**
Autre	1	3,29
Collecte	21	7,71
Conservation et retrait	7	5,58
Exactitude	2	6,58
Utilisation et communication	130	5,50
Total	**441**	**4,11**

* Plaintes en vertu de la LPRP fermées en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 26.

Tableau 3

Délais de traitement des plaintes en vertu de la LPRP – Enquêtes régulières, par type de plainte*

Type de plainte	Nombre	Délai de traitement moyen en mois
Accès	**124**	**20,86**
Accès	120	20,98
Correction ou annotation	2	8,42
Langue	2	25,63
Délais	**552**	**6,28**
Avis de prorogation	25	3,32
Délais	527	6,42
Protection des renseignements personnels	**91**	**23,41**
Collecte	15	20,78
Conservation et retrait	4	26,65
Exactitude	1	8,83
Utilisation et communication	71	23,98
Total	**767**	**10,67**

* Plaintes en vertu de la LPRP fermées en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 26.

Tableau 4

Délais de traitement des plaintes en vertu de la LPRP – Tous les dossiers fermés, par décision*

Type de plainte	Nombre	Délai de traitement moyen en mois
Plaintes ordinaires	**767**	**10,70**
Fondée et résolue	523	6,83
Non fondée	86	18,04
Abandonnée	86	16,44
Fondée	31	27,29
Réglée	23	23,81
Résolue	15	12,91
Hors du champ d'application	3	10,39
Résolue par règlement rapide	**441**	**4,11**
Total	**1 208**	**8,30**

* Plaintes en vertu de la LPRP fermées en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 26.

Tableau 5

Atteintes en vertu de la LPRP, par institution

Intimé	Incident
Affaires autochtones et du Nord Canada	4
Affaires mondiales Canada	3
Agence des services frontaliers du Canada	1
Agence du revenu du Canada	25
Anciens Combattants Canada	2
Bureau de l'enquêteur correctionnel	1
Centre de la sécurité des télécommunications Canada	1
Commission canadienne des droits de la personne	1
Commission de la fonction publique du Canada	6
Conseil de la radiodiffusion et des télécommunications canadiennes	1
Emploi et Développement social Canada	194
Gendarmerie royale du Canada	12
Immigration, Réfugiés et Citoyenneté Canada	7
Ministère de la Justice Canada	1
Ministère des Finances Canada	1
Monnaie royale canadienne	1
Office d'investissement des régimes de pensions du secteur public	1
Office national de l'énergie	1
Pêches et Océans Canada	3
Ressources naturelles Canada	1
Revera Inc.	1
Santé Canada	1
Secrétariat du Conseil du Trésor du Canada	2
Sécurité publique Canada	1
Service correctionnel Canada	4
Services publics et Approvisionnement Canada	3
Statistique Canada	3
Téléfilm Canada	1
Transports Canada	2
VIA Rail Canada	1
Total	**286**

Tableau 6

Plaintes et atteintes en vertu de la LPRP

Catégorie	Total
Acceptées	
Accès	300
Délais	698
Protection des renseignements personnels	256
Total des plaintes acceptées	**1 254**
Fermées à la suite d'un processus de règlement rapide	
Accès	221
Délais	59
Protection des renseignements personnels	161
Total	**441**
Fermées à la suite d'une enquête régulière	
Accès	124
Délais	552
Protection des renseignements personnels	91
Total	**767**
Total des dossiers fermés*	**1 208**
Atteintes signalées	
Accès non autorisé	22
Communication accidentelle	83
Perte	178
Vol	3
Total des atteintes signalées	**286**

* Plaintes en vertu de la LPRP fermées en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 26.

Tableau 7

Plaintes en vertu de la LPRP acceptées, par type de plainte

Type de plainte	Règlement rapide		Enquête		Nombre total	Pourcentage total
	Nombre	Pourcentage	Nombre	Pourcentage		
Accès						
Accès	216	49 %	75	9 %	**291**	**23 %**
Correction ou annotation	5	1 %	3	0 %	**8**	**1 %**
Langue	1	0 %			**1**	**0 %**
Délais						
Avis de prorogation			15	2 %	**15**	**1 %**
Correction – délais			1	0 %	**1**	**0 %**
Délais	56	13 %	626	77 %	**682**	**54 %**
Protection des renseignements personnels						
Autre	1	0 %			**1**	**0 %**
Collecte	18	4 %	27	3 %	**45**	**4 %**
Conservation et retrait	7	2 %	3	0 %	**10**	**1 %**
Exactitude	1	0 %	2	0 %	**3**	**0 %**
Utilisation et communication	135	31 %	62	8 %	**197**	**16 %**
Total*	**440**	**100 %**	**814**	**100 %**	**1 254**	**100 %**

* Les nombres ayant été arrondis, leur somme pourrait ne pas correspondre aux totaux indiqués.

Tableau 8

Les 10 institutions visées par le plus grand nombre de plaintes acceptées en vertu de la LPRP

Intimé	Protection des renseignements personnels		Accès		Délais		Total
	Règlement rapide	Enquête	Règlement rapide	Enquête	Règlement rapide	Enquête	
Service correctionnel Canada	27	18	33	7	24	331	**440**
Gendarmerie royale du Canada	16	14	37	22	12	131	**232**
Ministère de la Défense nationale	7	3	14	3	7	59	**93**
Agence des services frontaliers du Canada	10	13	25	9	5	14	**76**
Agence du revenu du Canada	20	7	18	2	1	15	**63**
Services publics et Approvisionnement Canada	8	2	4	1	3	31	**49**
Société canadienne des postes	8	5	9	2		9	**33**
Immigration, Réfugiés et Citoyenneté Canada	9		4	3	3	10	**29**
Service canadien du renseignement de sécurité	1		15	4		6	**26**
Emploi et Développement social Canada	7	2	7	5		3	**24**
Total	**113**	**64**	**166**	**58**	**55**	**609**	**1 065**

Tableau 9

Les 10 institutions visées par le plus grand nombre de plaintes acceptées en vertu de la LPRP, par exercice financier

Intimé	2014-2015	2015-2016	2016-2017	2017-2018
Service correctionnel Canada	314	547	389	440
Gendarmerie royale du Canada	140	120	160	232
Ministère de la Défense nationale	68	77	146	93
Agence des services frontaliers du Canada	66	88	107	76
Agence du revenu du Canada	106	85	65	63
Services publics et Approvisionnement Canada	9	10	25	49
Société canadienne des postes	32	17	19	33
Immigration, Réfugiés et Citoyenneté Canada	42	44	60	29
Service canadien du renseignement de sécurité	21	31	30	26
Emploi et Développement social Canada	35	42	36	24
Total	**833**	**1 061**	**1 037**	**1 065**

Tableau 10

Plaintes en vertu de la LPRP acceptées, par institution

Intimé	Règlement rapide	Enquête	Total
Administration canadienne de la sécurité du transport aérien	1	0	1
Administration portuaire de Québec	0	1	1
Affaires autochtones et du Nord Canada	7	8	15
Affaires mondiales Canada	0	2	2
Agence canadienne d'inspection des aliments	5	1	6
Agence de la santé publique du Canada	0	3	3
Agence des services frontaliers du Canada	40	36	76
Agence du revenu du Canada	39	24	63
Agence Parcs Canada	1	0	1
Agriculture et Agroalimentaire Canada	1	0	1
Anciens Combattants Canada	6	6	12
Banque du Canada	1	0	1
Bibliothèque et Archives Canada	7	1	8
Bureau de l'enquêteur correctionnel	2	0	2
Bureau du Conseil privé	2	0	2
Centre d'analyse des opérations et déclarations financières du Canada	2	0	2
Centre de la sécurité des télécommunications Canada	3	1	4
Comité de surveillance des activités de renseignement de sécurité	1	0	1
Commissariat à l'information du Canada	1	0	1
Commissariat à l'intégrité du secteur public du Canada	1	1	2
Commission canadienne des droits de la personne	2	2	4
Commission civile d'examen et de traitement des plaintes relatives à la Gendarmerie royale du Canada	0	7	7
Commission de l'immigration et du statut de réfugié du Canada	0	2	2
Commission de la fonction publique du Canada	1	1	2
Commission des libérations conditionnelles du Canada	5	0	5
Condition féminine Canada	4	0	4
Conseil de la radiodiffusion et des télécommunications canadiennes	3	1	4
Construction de Défense Canada	0	1	1
Diversification de l'économie de l'Ouest Canada	1	0	1
École de la fonction publique du Canada	1	0	1
Élections Canada	1	1	2

Intimé	Règlement rapide	Enquête	Total
Emploi et Développement social Canada	14	10	**24**
Environnement et Changement climatique Canada	0	1	**1**
Gendarmerie royale du Canada	65	167	**232**
Immigration, Réfugiés et Citoyenneté Canada	16	13	**29**
Innovation, Sciences et Développement économique Canada	2	3	**5**
Marine Atlantique S.C.C.	1	0	**1**
Ministère de la Défense nationale	28	65	**93**
Ministère de la Justice Canada	9	6	**15**
Office des transports du Canada	1	0	**1**
Office national de l'énergie	1	1	**2**
Office national du film du Canada	1	0	**1**
Pêches et Océans Canada	3	1	**4**
Ressources naturelles Canada	1	0	**1**
Santé Canada	6	3	**9**
Secrétariat du Conseil du Trésor du Canada	0	3	**3**
Sécurité publique Canada	3	0	**3**
Service Canada	3	2	**5**
Service canadien d'appui aux tribunaux administratifs	1	0	**1**
Service canadien du renseignement de sécurité	16	10	**26**
Service correctionnel Canada	84	356	**440**
Service des poursuites pénales du Canada	1	3	**4**
Services partagés Canada	2	0	**2**
Services publics et Approvisionnement Canada	15	34	**49**
Société canadienne des postes	17	16	**33**
Société Radio-Canada	3	1	**4**
Statistique Canada	2	2	**4**
Transports Canada	4	17	**21**
Tribunal des anciens combattants (révision et appel)	1	0	**1**
VIA Rail Canada	2	1	**3**
Total	**440**	**814**	**1 254**

Tableau 11

Plaintes en vertu de la LPRP acceptées, par province, territoire ou autre

Province, territoire ou autre	Règlement rapide		Enquêtes		Nombre total	Pourcentage total
	Nombre	Pourcentage	Nombre	Pourcentage		
Alberta	53	12,05 %	88	10,81 %	**141**	**11,24 %**
Colombie-Britannique	89	20,23 %	221	27,15 %	**310**	**24,72 %**
Île-du-Prince-Édouard	2	0,45 %	2	0,25 %	**4**	**0,32 %**
Manitoba	16	3,64 %	22	2,70 %	**38**	**3,03 %**
Nouveau-Brunswick	20	4,55 %	42	5,16 %	**62**	**4,94 %**
Nouvelle-Écosse	14	3,18 %	25	3,07 %	**39**	**3,11 %**
Nunavut	3	0,68 %	0	0,00 %	**3**	**0,24 %**
Ontario	164	37,27 %	211	25,92 %	**375**	**29,90 %**
Québec	60	13,64 %	158	19,41 %	**218**	**17,38 %**
Saskatchewan	1	0,23 %	21	2,58 %	**22**	**1,75 %**
Terre-Neuve-et-Labrador	6	1,36 %	10	1,23 %	**16**	**1,28 %**
Territoires du Nord-Ouest	1	0,23 %	3	0,37 %	**4**	**0,32 %**
Yukon	1	0,23 %	1	0,12 %	**2**	**0,16 %**
Non précisé	2	0,45 %	5	0,61 %	**7**	**0,56 %**
Autre (excluant les États Unis)	7	1,59 %	2	0,25 %	**9**	**0,72 %**
États-Unis	1	0,23 %	3	0,37 %	**4**	**0,32 %**
Total*	**440**	**100,00 %**	**814**	**100,00 %**	**1 254**	**100,00 %**

* Les nombres ayant été arrondis, leur somme pourrait ne pas correspondre aux totaux indiqués.

Tableau 12

Décisions en vertu de la LPRP, par type de plainte*

Type de plainte	Abandonnée	Hors du champ d'application	Non fondée	Résolue	Réglée	Fondée	Fondée et résolue	Résolue par règlement rapide	Total
Accès									
Accès	29	46	9	9	5	22	214	334	**334**
Correction ou annotation		1	1				7	9	**9**
Langue				2				2	**2**
Délais									
Avis de prorogation			4			1	20		**25**
Délais	35		9	2			481	59	**586**
Protection des renseignements personnels									
Autre								1	**1**
Collecte	1		8	1	1	4		21	**36**
Conservation et retrait	2	1			1			7	**11**
Exactitude			1					2	**3**
Utilisation et communication	19	2	17	2	10	21		130	**201**
Total	**86**	**3**	**86**	**15**	**23**	**31**	**523**	**441**	**1 208**

* Plaintes en vertu de la LPRP fermées en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 26.

Tableau 13

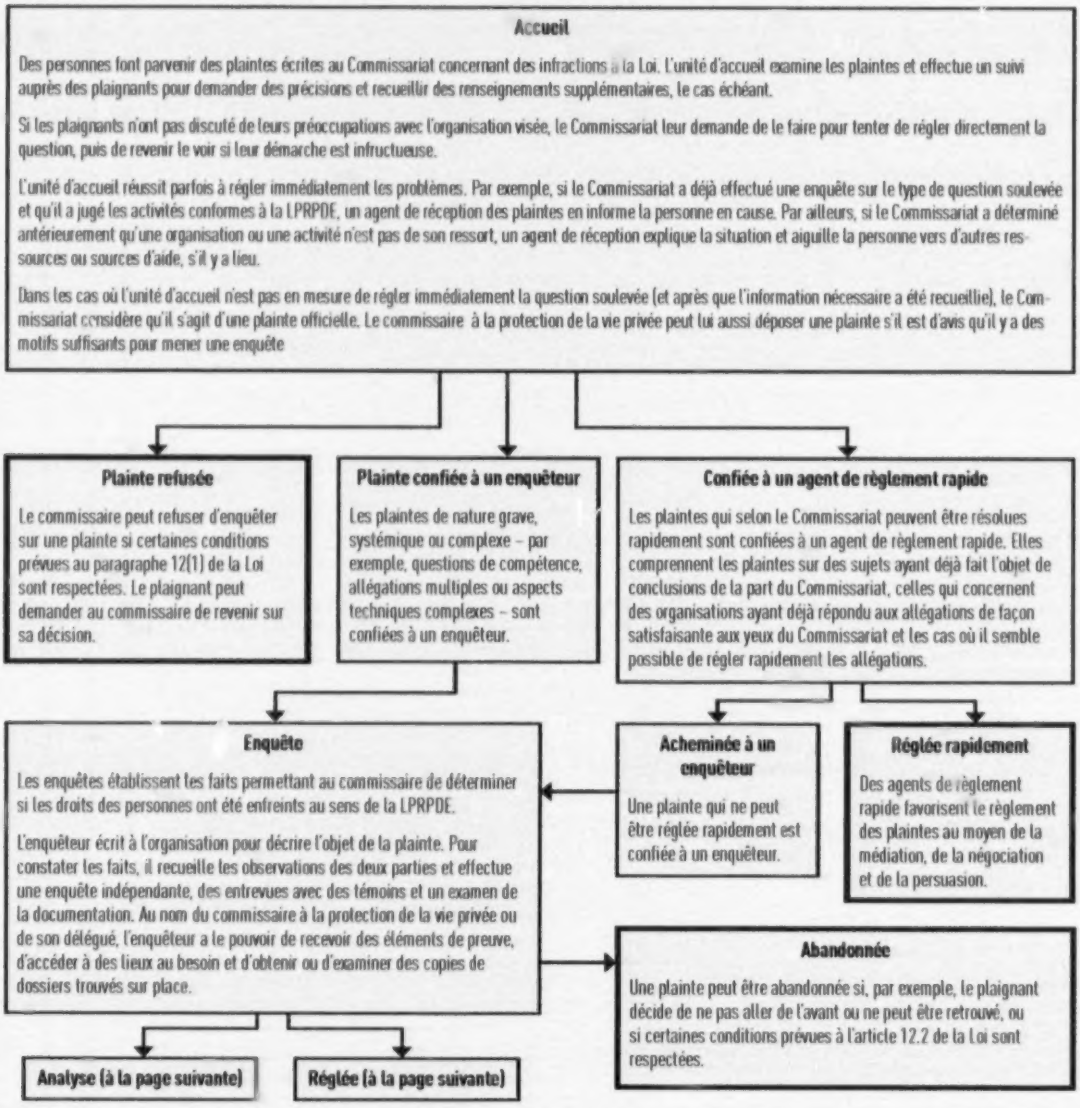
Décisions sur les plaintes relatives aux délais en vertu de la LPRP, par institution*

Intimé	Abandonnée	Non fondée	Résolue	Fondée	Fondée et résolue	Résolue par règlement rapide	Total
Affaires autochtones et du Nord Canada					1		**1**
Affaires mondiales Canada					1		**1**
Agence de la santé publique du Canada					1		**1**
Agence des services frontaliers du Canada		2			26	5	**33**
Agence du revenu du Canada					14	1	**15**
Anciens Combattants Canada					3		**3**
Commissariat aux langues officielles					1		**1**
Commission canadienne des droits de la personne					1		**1**
Commission civile d'examen et de traitement des plaintes relatives à la Gendarmerie royale du Canada					1		**1**
Commission de la fonction publique du Canada		1			1		**2**
Emploi et Développement social Canada	2	1			5	3	**11**
Environnement et Changement climatique Canada					5		**5**
Gendarmerie royale du Canada	1	1			73	12	**87**
Immigration, Réfugiés et Citoyenneté Canada	2		1		8	3	**14**
Innovation, Sciences et Développement économique Canada					2		**2**
Ministère de la Défense nationale		3	1		44	7	**55**
Ministère de la Justice Canada					3	1	**4**
Santé Canada					2		**2**
Secrétariat du Conseil du Trésor du Canada					1		**1**
Service Canada					1		**1**
Service canadien du renseignement de sécurité					3		**3**
Service correctionnel Canada	27	1			253	24	**305**
Service des poursuites pénales du Canada					1		**1**
Services publics et Approvisionnement Canada		2			34	3	**39**
Société canadienne des postes	2	1		1	3		**7**
Transports Canada	1	1			13		**15**
Total	**35**	**13**	**2**	**1**	**501**	**59**	**611**

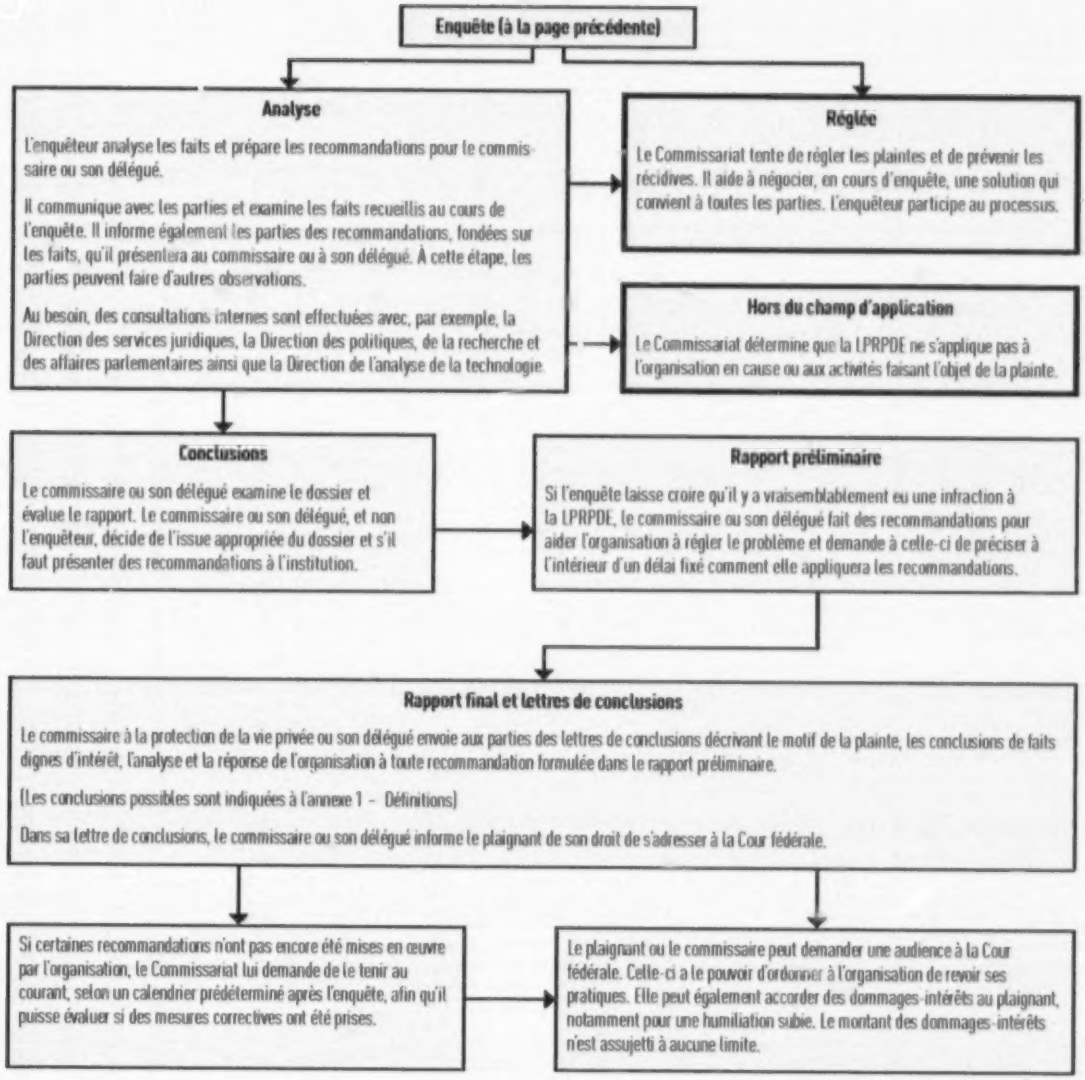
* Plaintes en vertu de la LPRP fermées en fonction d'une plainte représentative pour chaque série de plaintes similaires; le total des plaintes exclues équivaut à 26.

Annexe 3 – Processus d'enquête

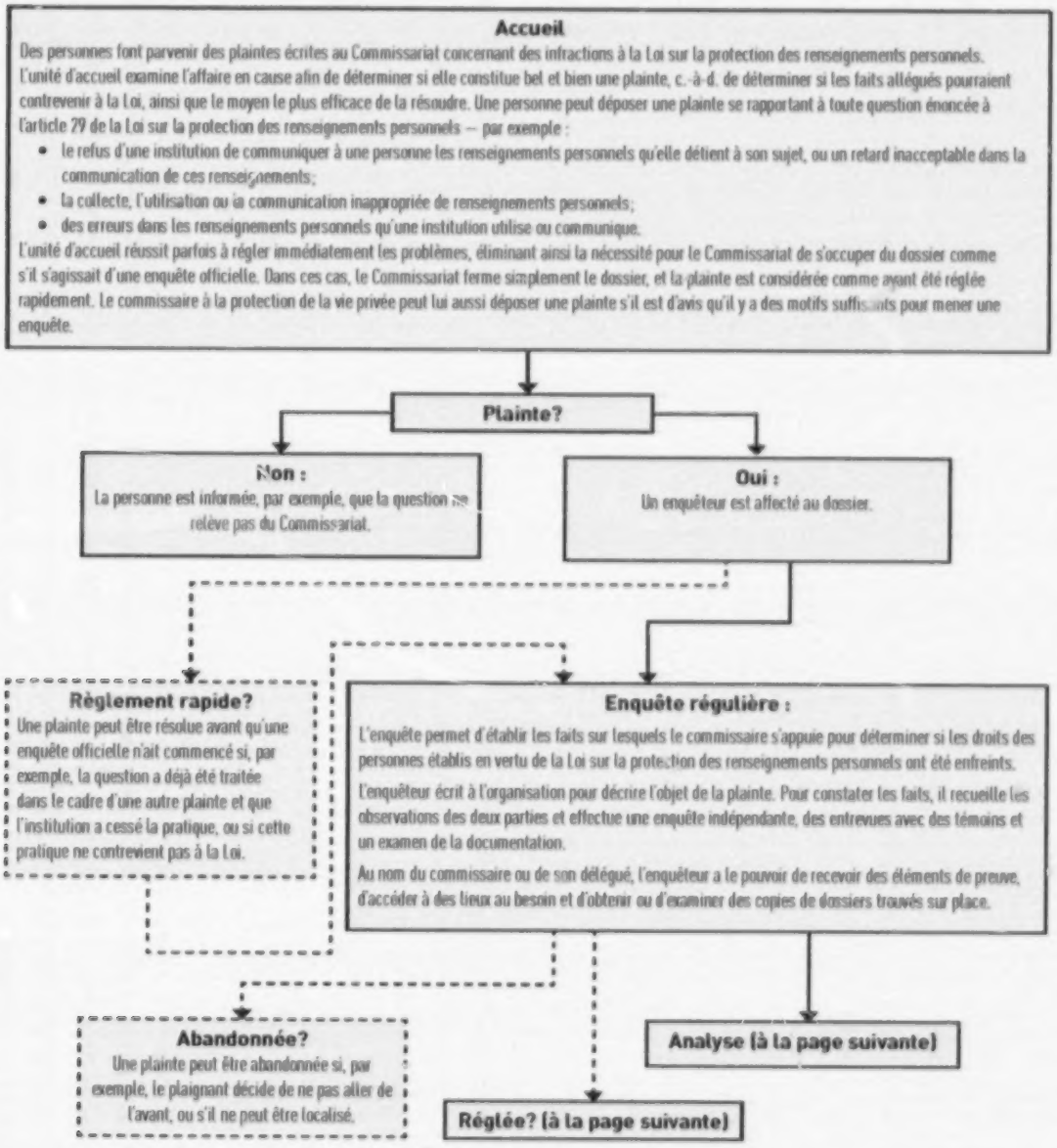
PROCESSUS D'ENQUÊTE EN VERTU DE LA LPRPDE



Processus d'enquête en vertu de la LPRPDE

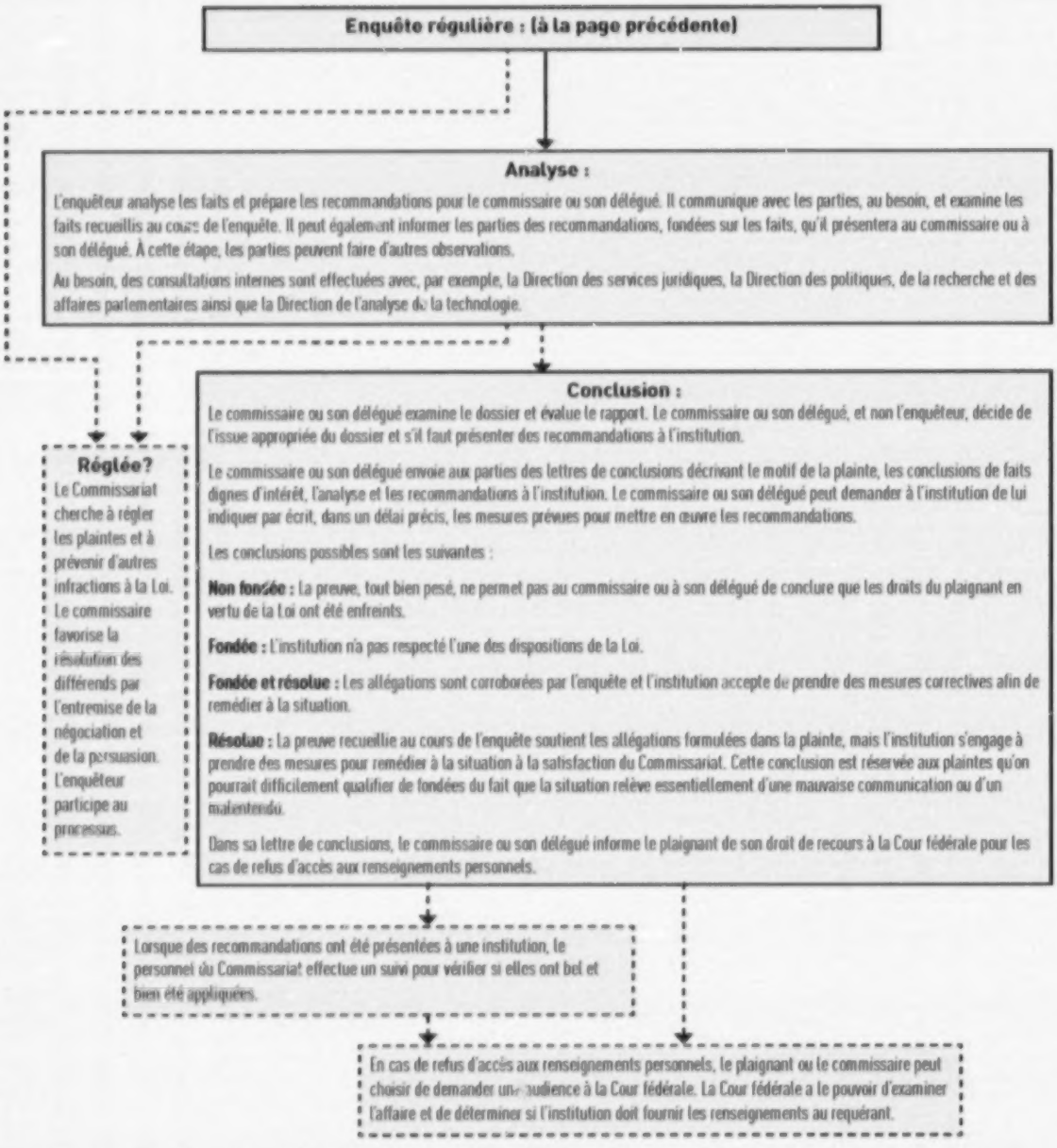


PROCESSUS D'ENQUÊTE EN VERTU DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*



Nota : Une ligne discontinue (- - - -) indique un résultat possible.

Processus d'enquête en vertu de la *Loi sur la protection des renseignements personnels*



Nota : Une ligne discontinue (- - - -) indique un résultat possible.

Annexe 4 – Rapport du commissaire spécial à la protection de la vie privée pour 2017-2018

J'ai le plaisir de rendre compte des activités du bureau du commissaire spécial à la protection de la vie privée dans le présent rapport. Depuis le 1er avril 2007, le Commissariat à la protection de la vie privée du Canada (CPVP) est assujetti à la *Loi sur la protection des renseignements personnels* (Loi). Il peut donc recevoir des demandes de renseignements personnels du fait qu'il s'agit d'une institution à laquelle s'applique le droit d'accès à ce type de renseignements.

La loi qui a apporté cette modification n'a toutefois prévu aucun mécanisme distinct de celui relevant du CPVP pour l'examen des plaintes selon lesquelles le CPVP n'aurait pas traité une demande de renseignements personnels conformément à la Loi.

Compte tenu d'un principe essentiel du droit de l'accès à l'information qui veut que les décisions sur la communication des renseignements gouvernementaux fassent l'objet d'un examen indépendant, on a créé le poste de commissaire spécial à la protection de la vie privée qui a le pouvoir d'enquêter sur les plaintes relatives au CPVP.

C'est pourquoi le commissaire m'a délégué la majorité des pouvoirs et des attributions qui lui sont dévolus en vertu des articles 29 à 35 et de l'article 42 de la Loi pour me permettre d'enquêter sur les plaintes en vertu de la *Loi sur la protection des renseignements personnels* déposées contre le CPVP.

Plaintes de l'exercice précédent non réglées

Notre bureau n'avait aucune plainte en suspens depuis l'exercice précédent.

Nouvelles plaintes déposées au cours du présent exercice

Deux plaintes ont été reçues cette année. Elles ont toutes fait l'objet d'une enquête et ont été réglées avant la fin de l'exercice.

La question soulevée dans la première plainte concernait un refus d'accès. Le CPVP avait répondu au demandeur que tous les documents lui avaient déjà été fournis dans le cadre d'une demande précédente de renseignements personnels. Insatisfait de cette réponse, le plaignant a allégué que le CPVP n'avait pas effectué de recherche exhaustive et qu'il devait bien exister de nouveaux documents.

L'enquête que j'ai menée a permis de conclure que le CPVP avait effectivement fourni tous les documents appropriés dans le cadre d'une demande antérieurement présentée par le plaignant et qu'aucun nouveau renseignement n'existait. Par conséquent, j'ai conclu que cette plainte n'était pas fondée.

La deuxième plainte concernait l'application des dispositions du paragraphe 22.1(1) de la Loi, selon lesquelles le CPVP est exempté de communiquer les renseignements obtenus ou préparés dans le cadre d'une enquête. Cependant, une fois l'enquête et toutes les procédures connexes terminées, cette exemption est levée en partie. À ce stade, l'exemption ne s'applique plus aux documents créés durant l'enquête.

Mon enquête a révélé que les documents contestés avaient été obtenus au cours des propres enquêtes du CPVP. J'ai donc conclu que l'organisme avait appliqué cette exception obligatoire à juste titre lorsqu'il avait refusé de communiquer les documents demandés. Par conséquent, la plainte n'était pas fondée.

Outre ces deux plaintes, le commissaire spécial a reçu de la correspondance d'un certain nombre de personnes qui n'étaient pas satisfaites de la manière dont le CPVP avait traité leur plainte sous-jacente ou qui étaient insatisfaites que le CPVP n'ait pas, selon elles, traité promptement leurs plaintes.

Le commissaire spécial n'a pas compétence pour enquêter au sujet des préoccupations concernant la façon dont le CPVP a mené enquête sur des plaintes qui lui ont été présentées à titre d'organe de surveillance en vertu de la Loi. En outre, mon bureau ne peut pas non plus enquêter au sujet du retard du CPVP dans le traitement de telles plaintes. Notre mandat se limite à recevoir des plaintes selon lesquelles le CPVP aurait mal géré lui-même les renseignements personnels dont il a la garde, et à faire enquête sur ces plaintes.

Conclusion

L'existence du commissaire spécial, qui occupe une fonction indépendante, permet de veiller à l'intégrité du traitement des demandes de renseignements personnels présentées au CPVP en tant qu'institution, et contribue ainsi au système global d'accès à l'information à l'échelle fédérale. Mon bureau continuera de jouer ce rôle en matière d'accès à l'information.

David Loukidelis (c.r.)
Commissaire spécial pour le
Commissariat à la protection de la vie privée du Canada

Mars 2018